

Cyber Code of Conduct

Name of document author:	Ben Everitt
Job title of document author:	Acting Head of IT
Division responsible for document:	Resources
Date document written:	-
Date of last revision:	December 2011
Approving committee:	IG Steering Group
Date approved by approving committee:	29 th March 2012
Next due for revision:	29 th March 2013
For use in:	Trust wide
For use by:	All Staff
Keywords:	Cyber Code, IT, Conduct
Compliance links:	N/a

Version Information

Version No	Updated By	Date of Update	Description of Change to this Version
10.1	Ben Everitt	29/12/2011	Policy reviewed and updated
10.1	Mark Rundle	30/12/2011	Document reviewed and amended accordingly
10.1	Chrissy Jackson	29/03/2012	Policy approved by the IG Steering Group

TABLE OF CONTENTS

Section	Page
CYBERCODE OF CONDUCT	
1	MANAGEMENT SUMMARY..... 1
2	POLICY KEY POINTS 1
3	INTRODUCTION..... 3
4	SCOPE OF POLICY..... 4
5	EMAIL HARASSMENT 5
6	AUTHORISED USE 6
7	NON-AUTHORISED USE..... 6
8	CONFIDENTIALITY 8
9	FREEDOM OF INFORMATION 9
10	USE OF THE TRUST NAME 9
11	INTELLECTUAL PROPERTY 9
12	LEGAL MATTERS 10
13	USER REGISTRATION..... 10
14	USER RESPONSIBILITIES..... 10
15	IT DEPARTMENT RESPONSIBILITIES 11
16	GOOD PRACTICE GUIDE 12
17	FILTERING 12
1	INTRODUCTION..... 1
2	INAPPROPRIATE USE..... 1
3	GOOD EMAIL PRACTICE 2
4	GOOD INTERNET PRACTICE 5
5	EMAIL FILTERING RULES..... 6
6	INTERNET FILTERING RULES..... 8

7 GLOSSARY 9

LINK TO [GOODPRACTICE](#) GUIDE

LINK TO [FRAUD AND CORRUPTION POLICY](#)

1 MANAGEMENT SUMMARY

- 1.1 In common with all comparable public and private sector organisations, the Trust has increasingly come to rely upon its IT systems and related services to support its normal day to day business operations especially in the delivery of patient care. These IT systems and services are at constant risk from virus, spyware, adware, malicious software attacks and intentional/unintentional internal breaches. The Trust wishes to ensure that these systems and services are operated in accordance with the purposes for which they have been made available and to do so in a way that does not compromise patient safety and staff welfare and also complies with current legislation on these matters.
- 1.2 The IT department has been entrusted to ensure, that measures are in place to protect against potential threats and damage from any untoward incident that may occur. This code of conduct deals with use of the Trust email, Internet/Intranet and related communication systems.
- 1.3 The Trust email system is the main method for Trust communications and all staff are obliged to use this system in line with the requirements set out in this and companion policies. The use of personal email and non-Trust authorised systems for conducting the normal business of the Trust is not permitted.
- 1.4 This policy document supersedes the current CyberCode (version 9) but includes any provision from the current CyberCode (version 9) that has not been further commented on in this policy.

2 POLICY KEY POINTS

- 2.1 Some of the key points of this updated policy follow and are commented upon in more detail in the main document.

Harassment

- 2.2 The Trust's IT systems and assets must not be used in any way to harass staff, patients or any member of the general public. Harassment is a criminal offence and any attempt to use the system to harass others could lead to Trust disciplinary action being instigated and potential legal proceedings.

Authorised Use

- 2.3 The Trust's IT systems have been implemented primarily for the execution of Trust business but the Trust does permit reasonable personal use of these facilities provided the individual's ability to meet their contractual obligations is not affected and the terms set out in this

policy are adhered to. Authorised use is covered in more detail in [Section 4](#).

Non-authorised Use

- 2.4 The Trust systems must never be used to access inappropriate sites or sites deemed to contain offensive material. Inappropriate or offensive material must not be transmitted by email, the Internet or any other electronic transmission medium. Non-authorised Use is covered in more detail in [Section 5](#).

Confidentiality

- 2.5 It is of paramount importance that the Trust business is maintained in confidence at all times. This extends to ensuring that patient data is never knowingly compromised, for example, by the electronic transfer of patient or patient-related data by non-approved email or other communication systems. The NHS has put in place a secure NHS Mail system that allows confidential patient or other sensitive information to be passed between NHS employees and other authorised parties.

System Monitoring

- 2.6 The Trust monitors the use of its IT systems and services to help ensure that they are used in accordance with Trust policy and legal requirements. This monitoring is carried out using sophisticated monitoring software which is configured to monitor activity (without human intervention) and to report only on exceptional activity that may contravene the Trust policy.

System Usage

- 2.7 A companion document is attached to this policy which is entitled: [A Good Practice Guide to using Email and Internet in the Workplace](#). This document sets out guidelines for obtaining best use of these systems and also limitations to their use. This guide has been produced in line with industry best practice and will be periodically updated to reflect changing best practice.

3 INTRODUCTION

- 3.1 The Norfolk and Norwich University Hospital NHS Trust ('the Trust') like many other organisations, has invested heavily in the deployment of sophisticated Information Technology (IT) systems and services to assist both in the delivery of high quality patient care and the administration associated with the delivery of this care. The effectiveness of this deployment has resulted in a high degree of reliance on these systems and services being available on a 24/7 continuous basis so that the Trust can meet its obligations to its patients and staff alike.
- 3.2 To ensure that these obligations continue to meet the agreed specified criteria, policies and guidelines have been developed in line with best industry practice, current legislation and Trust internal auditor requirements for all staff to observe and work within. Policies of this type are designed to ensure that the Trust systems are operated for the benefit of patients and staff and to minimise the opportunity for these systems to be used for other purposes including (but not limited to): excessive personal use; access to and uploading/downloading of inappropriate material; harassment; sex/racial discrimination etc. The Trust, therefore, has a duty to ensure that controls are in place to minimise the risk of potential security breaches or other negative consequences.
- 3.3 Staff will be notified of these policies on joining the Trust and be kept up to date with news of modifications, and new policies via the Trust's email and Intranet systems.
- 3.4 The Trust will regularly review these policies to ensure their appropriateness, relevance and their compliance with current legislation, industry best practice and Trust internal auditor requirements.
- 3.5 This policy covers the use of Trust provided computer equipment (including but not restricted to PCs and laptops), Internet and Intranet access and use, and internal and external email access and use. Breach of any of the restrictions below could result in the instigation of the Trust's Disciplinary procedures and could give rise to criminal and/or civil liability. Fraudulent or serious misuse of the system could in certain circumstances amount to gross misconduct. Any suspected fraudulent use or serious misuse of Trust computer equipment must be referred in the first instance to the Head of IT for investigation and potential escalation to the Local Counter Fraud Specialist.

4 SCOPE OF POLICY

- 4.1 The purpose of this policy and associated guidelines is to clearly define the permissible and recommended use of the Internet, Intranet and internal/external email systems by authorised Trust staff. This policy also covers staff who are not employed by the Trust, but whom the Trust has granted access.
- 4.2 The policy and its associated guidelines cover:
- Email Harassment
 - Authorised Use
 - Non-authorised Use
 - Confidentiality
 - Use of the Trust Name
 - Intellectual Property
 - Legal Matters
 - User Registration
 - User Responsibilities
 - IT Department Responsibilities
 - Good Practice Guide
 - Filtering Process

5 EMAIL HARASSMENT

- 5.1 This section sets out in more detail the implications of using the email and Internet system(s) for potential harassment of recipients.
- 5.2 It is essential that all users are aware of the potential for harassment to occur via emails or Internet facilities such as chat rooms or social networking sites that could then result in a discrimination claim. The same rules apply here as to any other form of harassment. So, if an email or other electronic communication amounts to treating an individual less favourably than another due to their sex, race, age, or because of a disability, and this results in a detriment to that individual, then an act of discrimination will have occurred. This is the case, regardless of the intention.
- 5.3 Where an employee carries out an act of harassment or discrimination in the course of their employment, the employer is vicariously liable for that act - even when the act is unauthorised. In order to defend a discrimination claim, the employer has to show that it took all reasonably practicable steps to prevent the employee(s) from carrying out the discriminatory act.
- 5.4 This highlights the importance and the need for employers to be able to monitor the use of emails and other electronic transmissions. In order to do so, it is essential an employer has clear policies and guidelines in place. For example, once an issue of email harassment has been raised and the harasser identified, immediate action will be taken to stop the harassment and instigate the disciplinary procedure in line with the Trust policy on harassment while supporting the allegedly harassed employee.
- 5.5 This area is particularly significant in view of the scope for emails to reach a more extensive audience with the use of the 'forward' facility. It is likely that, in the same way that motive is irrelevant, the fact that others were not supposed to see the email will be irrelevant and that the initial distribution of the information will be sufficient for a claim of discrimination to be made with potential liability for the Trust.
- 5.6 It is clear from the above that the Trust would wish to ensure that there are no occasions where the system is used knowingly or unknowingly to harass staff, patients or other intended recipients and as such the Trust wishes to ensure that all staff are aware of the potential for harm and the possible consequences to those involved in this activity.
- 5.7 Harassment is a recognised criminal offence and it is possible for staff who may have been harassed to instigate legal proceedings against any member of staff accused of such harassment.

6 AUTHORISED USE

General

- 6.1 Access to the IT systems and services covered in this policy is granted for the execution of Trust business and must be carried out in line with the provisions contained in the [Trust IT Security Policy](#).
- 6.2 The Trust permits reasonable personal use of these systems provided this does not interfere with the ability of individuals to meet their contractual and other commitments and that any personal use is governed by the requirements of this policy.
- 6.3 Personal access to the Internet can be limited or denied by the Trust with Trust decisions being final.

File Downloads

- 6.4 File downloads must be carried out in accordance with the laws which protect copyright, designs and patents including licensing laws and must not present a security threat and must be authorised by the IT department before a download is attempted. Further detailed guidance on this can be obtained from the IT department Helpdesk.

7 NON-AUTHORISED USE

The Internet (or any facility available within the Internet (including but not limited to web based email systems) must never be used for the communication of patient or confidential information. The Internet has not been designed as a secure communication medium. Therefore, it should be noted that the Trust email system is intended to be used for general communication and can only be used to transmit patient or other confidential or sensitive information if appropriate approval has been obtained and email encryption applied.

Note: Patient and or confidential information can be transmitted securely via the NHS Mail system. Please contact the IT Helpdesk for further details.

- 7.1 The following paragraphs sets out what the Trust Internet, Intranet, email and related systems must **NOT** be used for:
- visiting Internet sites that contain, but not limited to, obscene, hateful, violent or pornographic material;
 - No member of staff is permitted to access, display, use, distribute disseminate or upload/download to/from Internet sites that store offensive or unauthorised material. Doing so is considered a serious breach of this policy and could result in formal disciplinary action being taken against any individual suspected of such

breaches. Examples of offensive material includes: hostile text; images relating to age, gender, ethnicity, race, violence, sex, sexual orientation; religious or political beliefs and disability. This list is not intended to be exhaustive and does not preclude access to sites for clearly demonstrable clinical reasons;

- using the computer to perpetrate any form of fraud, or software or music piracy;
- using the Internet to download streaming data, video, TV or radio channels; unless of an educational nature pertaining to work orientated uses
- using the Internet or email system to send offensive or harassing material to other users;
- downloading software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence and by express permission of the Trust;
- Hacking into unauthorised areas;
- Creating or transmitting defamatory material;
- Introducing any form of computer virus or other damaging software into the Trust network;

EMAIL SPECIFIC

- Use of NNUH communications systems to set up personal businesses or send chain letters;
- Forwarding of NNUH confidential messages or information to external locations;
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;
- Distributing, disseminating or storing images, text or materials that might be considered offensive or abusive, in that the context is a personal attack, sexist or racist;
- Accessing copyrighted information in a way that violates the copyright;
- Breaking into the system or unauthorised use of a password/mailbox;

- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters;
 - Transmitting unsolicited commercial or advertising material;
 - Undertaking deliberate activities that waste staff effort or networked resources, for example, but not limited to, the distribution of chain letters, spam or other material not permitted by this policy;
 - It is a breach of the policy to upload/download files that could disable the network or that have the ability to compromise the integrity and security of the networks and associated peripherals. It should also be noted that it is an offence under the terms of the [Computer Misuse Act 1990](#) to intentionally introduce files or programs capable of causing computer problems and potential disruption and any action capable of compromising system integrity and information confidentiality.
 - Introducing any form of computer virus into the Trust network;
- 7.2 Other than instances that may lead to criminal prosecution, the final arbiter on what constitutes offensive material will be senior Trust management as outlined in the Trust's disciplinary policy where this is not defined by law.

8 CONFIDENTIALITY

- 8.1 Users are bound by the terms of the [Trust's Confidentiality and Security Policy](#).
- 8.2 Under the *Data Protection Act* users may not disclose any information relating to an identifiable individual. Additionally, they may not disclose confidential information relating to any aspect of the business of the NHS. (A summary of the main provisions of the *Data Protection Act* is available on the Trust Intranet: via [Data Protection Act Summary](#))
- 8.3 The following should be taken into account when using email to send confidential information:
- 8.3.1 Users should ensure that both they and the party with whom they are communicating understand the risks of using email as a communication channel and agree what will and will not be sent.
- 8.3.2 Where email messages do contain confidential information they should be clearly marked 'Confidential'.
- 8.4 All email sent from Trust's email systems will be automatically and electronically 'stamped' with a disclaimer in the event that they reach anyone other than the intended recipient.

9 FREEDOM OF INFORMATION

- 9.1 Users should note that under the [Freedom of Information Act 2000](#) emails may become public documents if the contents are deemed to be in the public interest.

10 COUNTER FRAUD

- 10.1 Users are bound by the terms of the [Trust's Fraud and Corruption Policy](#).
- 10.2 All employees have a personal responsibility to protect the assets of the Norfolk and Norwich University Hospital NHS Trust, including all buildings, equipment and monies from fraud, theft, corruption or any other irregularity.

11 USE OF THE TRUST NAME

- 11.1 Unless they are currently authorised to do so, users are not permitted to write or present views on behalf of any part of the Trust via any part of the Internet, Intranet or email.

12 INTELLECTUAL PROPERTY

- 12.1 All staff are reminded that material displayed on the Internet may be subject to copyright restrictions. Many organisations presenting information over the Internet have become sensitive to breaches of their copyright and have taken action against the perpetrators. Contrary to popular belief, Web pages are not automatically in the public domain and are subject to the same usage restrictions as printed material.
- 12.2 Unless you are absolutely sure that the owner of material displayed on the Internet has given permission for using their material, it should not be copied. Where an owner does provide permission for taking copies for personal use, their restrictions on usage must be followed. In no circumstances should material copied from the Internet be included in our own Web pages or other publications, unless the copyright rules have been followed.
- 12.3 In general terms small amounts of copyrighted material can be used in quotations, provided that the source is explicitly stated. In other cases it may be necessary to gain permission from the owner for use of their material.
- 12.4 Failure to comply with copyright rules could lead to the Trust being involved in court action and anyone found infringing copyright could be subjected to disciplinary action. If you are uncertain about the

copyright position relating to any material available on the Internet you should avoid its use until such time as the position has been clarified.

13 LEGAL MATTERS

- 13.1 Email messages can form contractual documents that are legally binding on the Trust. They are also admissible as evidence in a court of law. It is therefore vital that they contain accurate information and that they do not inadvertently commit the Trust in any way, which is not specifically intended. Headings such as 'without prejudice', 'draft' etc should be used in emails in the same way as on letters or faxes.
- 13.2 Where the contents of an email message may be required for legal purposes, the message should also be sent securely to the addressee(s) in hardcopy (letter) form and a separate hardcopy kept on the file.
- 13.3 The Internet email address of the recipient or sender is not sufficient for legal purposes. The full name and contact details of the Trust should appear within the body of all emails.
- 13.4 It is not permissible to offer a prospective applicant employment via email.
- 13.5 If users have concerns over the legal status of an intended message they should discuss their concerns with their immediate manager.

14 USER REGISTRATION

- 14.1 Each new member of staff who requires access to the Internet, Intranet and email systems will be issued with account registration and password details on joining the Trust. Registration details will be passed to new users during their induction.
- 14.2 All users are contractually bound by this and other Trust policies and any changes that may be made to them from time to time.

15 USER RESPONSIBILITIES

- 15.1 Authorised users are responsible for keeping their password confidential. Users **must not** divulge their password to any other users. For example, password details should **not** be retained on paper and be readily accessible to others.
- 15.2 Use of the email system should improve the communication process and not detract from it. Communications should always be sent to the appropriate person and not be copied unnecessarily to others in the Trust. Users should consider whether the recipient really requires the information and the detail contained within the message.

- 15.3 It is prohibited for users to originate or distribute 'chain' letters or 'spam' by email. If a user receives a chain or spam message they should delete it and inform the IT Helpdesk.
- 15.4 In the unlikely event that a user is unintentionally connected to a site, which contains inappropriate material, then the user must immediately disconnect from the site and inform the IT Helpdesk.
- 15.5 Users are not permitted without express permission of the IT department to create their own Internet or Intranet sites on any part of the Trust IT infrastructure.

16 IT DEPARTMENT RESPONSIBILITIES

- 16.1 The IT department is responsible for ensuring that all of the Trust's communications systems are operated in a way that fully meets the terms and conditions of the [NHS Code of Connection](#). The NHS Code of Connection is the set of rules set up by the NHS to govern how NHS organisations are permitted to use the NHS network that is intended to facilitate the electronic transmission of all communications between NHS users.
- 16.2 The IT Department, acting on delegated authority from the Chief Executive, is responsible for maintaining a safe and secure computing environment in the Trust.
- 16.3 The Trust has charged the IT Department with monitoring use of the Internet, Intranet and email systems to ensure that all use complies with the requirement of this policy, current legislation and internal auditor requirements. This monitoring is not carried out by staff. To this end, software monitoring systems are in operation to help ensure that use is regulated within the requirements of the policy. Monitoring is operated on an 'exception' basis and there is no routine monitoring of normal system use. This monitoring includes (but is not limited to):
- Recording of unauthorised access attempts
 - Excessive time spent on Internet and related sites
 - Repeated attempts to access inappropriate sites
 - Identification of material likely to cause offence or breach confidentiality or security requirements
 - Identification of file and other data uploads/downloads
 - Black listed email senders known as Spammers
 - Virus detection
 - Adware, spyware and other malicious software

- 16.4 If there are reasons to suspect that any of the above conditions are violated then the Trust may instigate an investigation that could lead to formal disciplinary action being taken against an individual(s).

17 GOOD PRACTICE GUIDE

- 17.1 A [good practice](#) guide is attached to this policy that sets out how the Trust wishes to see its email, Internet and related systems used. This guide will help to ensure that the systems are being used in an optimum and safe way that complies with the requirements of this policy and current legislation.

18 FILTERING

- 18.1 There are many sophisticated software monitoring systems in the market that can help to ensure that an organisation's policy requirements are adhered to. The Trust uses such a system.
- 18.2 The system deployed allows the automatic monitoring of emails and web accesses to ensure that the policy rules are adhered to. These rules are set out in the best practice guide and may change from time to time. Any changes to the Cybercode will be notified to users and the latest update copy of the Cybercode will be available on the Trust Intranet.
- 18.3 The monitoring software automatically checks for rules compliance, individuals are not responsible for this activity. When a rule is breached, the system will notify the intended recipient and if the reported breach is incorrect for any reason then the intended recipient will be able to request that a 'quarantined' email is released to them.
- 18.4 There are rules in place to monitor content of emails but this is restricted to incoming/outgoing emails only. The content of internal email is not monitored by the system or in any other way. This monitoring is system based and not carried out by staff.

A Good Practice Guide To Using Email And Internet In The Workplace

Author: Head of IT
Department:: IT
Revision Date: December 2011
Version: 10.1

TABLE OF CONTENTS

Section	Page
1 INTRODUCTION.....	1
2 INAPPROPRIATE USE.....	1
3 GOOD EMAIL PRACTICE	2
4 GOOD INTERNET PRACTICE	5
5 EMAIL FILTERING RULES.....	6
6 INTERNET FILTERING RULES.....	8
7 GLOSSARY	9

1 INTRODUCTION

- 1.1 In today's NHS environment, email is second only to voice as the preferred method of communication and is the most used software application in many organisations. In the Trust, this expansion in the use of email and the Internet has meant that all staff have access to these facilities. The Trust is concerned to ensure that its email, Internet and related systems are operated in an optimum way, in line with its policies on these matters and in compliance with current legislation on these matters and consequently has produced this guide to best operating practice.
- 1.2 The guide also sets out the email and Internet 'filtering rules' that the Trust has in place to help ensure that appropriate and optimum use is made of the system. A glossary is also included to explain some technical terms.

2 INAPPROPRIATE USE

- 2.1 The Trust wishes its email, Internet and related systems to be used in a way that supports the normal business of a hospital. Trust senior managers are concerned about the potential risks that the Trust staff and patients are potentially exposed to resulting from inappropriate use of these systems. Dangers include:
- The sending of inappropriate content that can jeopardise the legal integrity of the Trust and/or patient confidentiality;
 - The introduction of viruses, spyware, adware and other malicious software into the Trust network of computers;
 - Claims for harassment or different forms of discrimination against members of its staff and/or colleagues;
- 2.2 The expansion in the use of email has grown hand in hand with the use of the Internet. The Internet has become a valuable source of information. Most users of the Internet are unaware of the potential implications and risks (potential harassment, discrimination and employers being compromised by staff etc.)
- 2.3 This document provides a best practice guide to using email, Internet and related systems provided by the Trust to help staff carry out their normal business activities. It will also help ensure that the Trust's policies, current relevant legislation and internal auditor requirements are adhered to.
- 2.4 All users should be aware that, depending on the circumstances, email content is subject to rules of disclosure and therefore, inserting terms

like 'internal use' and 'confidential' will not ensure that email content is kept private.

3 GOOD EMAIL PRACTICE

- 3.1 This section sets out a guide to the best industry practice in the efficient and proper use of the email system. The following lists set out the do's and don't of use and is not intended to be exhaustive.

Security

- 3.2 Do not open attachments from unknown senders – delete them. Opening unsolicited attachments is the most common method for the transmission of destructive computer viruses and other types of malicious software.
- 3.3 Be wary of odd subject lines e.g <For you> < ID 12345 > < Your photos >. Again unfamiliar email address with unfamiliar subject lines could be a potential virus so do not open them, instead delete them
- 3.4 Be cautious of files downloaded from [HTML](#) formatted emails. HTML emails look like web pages with links that can be clicked on. When clicking on HTML links within an HTML email it could download a potential virus or other malicious software.
- 3.5 Junk email also known as [SPAM](#) and chain letters can also contain viruses so don't open them or send them on – delete them.
- 3.6 Only send an attachment if requested or needed; do not send unnecessary attachments as this requires extra network capacity and could be a virus concern for the recipient.
- 3.7 Beware of emails with 'plausible' credentials asking for personal details such as bank information. Ensure that all suspicious emails are forwarded to the Trust's IT Security Manager for analysis and investigation prior to being deleted. If appropriate, relevant emails may subsequently be forwarded to the Local Counter Fraud Specialist.
- 3.8 Do not under any circumstances use the Trust email system to send patient confidential information to external recipients. If patient confidential information is required to be sent to an authorised NHS user then the NHS email system must be used as it has been designed to ensure the safe and confidential transmission of such material.
- 3.9 Do not use the Trust or any other email system to transmit patient or confidential information to any other email system, eg, Yahoo, AOL etc.

3.10 Confidentiality

-
- 3.11 The identity of an email sender can be faked which is known as **spoofing**. If you receive an apparently legitimate email requesting sensitive information including (but not limited to) patient confidential data, make sure you get verbal confirmation of the request before sending a response via the Trust approved email system. If in doubt, refer any suspicious emails to the Trust's IT Security Manager to undertake further enquiries to validate any request. Where appropriate, relevant emails may be forwarded to the Local Counter Fraud Specialist for investigation.
- 3.12 Use appropriate and authorised methods to send sensitive patient data to other organisations. Using email to other non NHS organisations could result in the email being intercepted. Only email to other NHS sites via NHSnet email accounts or send the information via the post.
- 3.13 Ensure that sensitive internal documents are always marked with an appropriate phrase like 'For Internal use only'. If sensitive documents are not marked with appropriate phrase then the recipient could unknowingly pass on confidential information without being aware.
- 3.14 Check the recipient list when replying to an email as sometimes there could be someone who is not authorised to receive it.
- 3.15 **Housekeeping**
- 3.16 Automatic housekeeping procedures are in place to manage the total capacity used by the email and related systems. Every three months mail items in the 'send and deleted' folders will be automatically deleted.
- 3.17 Delete joke emails so that capacity on the email system can be managed efficiently and do not forward them on. Many joke emails contain content that can be construed to violate the terms of this policy.
- 3.18 **Legal**
- 3.19 Remember that email carries an implied Trust letterhead so beware any emails can be interpreted as representing the Trust and can be legally binding. An email carries the same legal status as a letter carrying the Trust letterhead.
- 3.20 Any discussion, views or quotes using the Trust email system could lead to a lawsuit which can be potentially very damaging.
- 3.21 Only send what you have the legal right to pass on. Sending unidentified copyright material could lead to legal action.
- 3.22 **Etiquette**
- 3.23 Use upper and lower case letter as in a normal sentence. Don't use all caps as this is considered SHOUTING.

-
- 3.24 Your signature file should contain your name and contact details without using fancy fonts. Signatures containing HTML code or images can be lost by some email systems.
 - 3.25 The practice of using a 'facsimile' signature in emails is discouraged as it implies but does not have any legal status.
 - 3.26 Use the 'urgent' flag and 'follow up' flag only to verify that an important action has been carried out. Don't use the flags too often otherwise they tend to get ignored.

4 GOOD INTERNET PRACTICE

- 4.1 This section sets out a guide to the best industry practice in the efficient and proper use of the Internet.
- 4.2 **Finding Web sites**
- 4.3 Once you are able to connect to the Internet, the next step is to be able to move about (surf). The main way to do this is by using the World Wide Web (www) and the web sites on it. The main way to get about on the Internet is by using hyperlinks, hyperlinks are pictures or text that you click on and they then send you to another web site / page address etc. The best way to find hyperlinks that interest you are by using search engines and directories. Search engines allow you to search online databases of web sites and directories lists of web sites for certain categories.
- 4.4 Search engines include: Google, Fast, AskJeeves - Teoma, Yahoo etc.
- 4.5 **Basics of Searching**
- 4.6 Using a search engine is very simple, all you have to do is enter a keyword or keywords into the search box and click the 'enter' or 'search' button. The most important part of a search is to pick the right keywords, always pick the most relevant keyword. For search engines such as Google (currently the most popular search engine) it is useful to remember the following points.
- 4.7 The keywords entered first are the keywords deemed most important.
- 4.8 Common words such as "where" and "how" are not recognised and are ignored.
- 4.9 If the character "+" (leave a space in front of "+") is put in front of a keyword it indicates the keyword is essential.
- 4.10 The best way for searching for a phrase is to put quotation marks around the keywords e.g. "Clinical treatment".
- 4.11 **Domain Names**
- 4.12 Domain Names are the unique addresses of web pages. The domain name of a web page usually gives an indication of the content residing there. Domain names also have an extension, examples of these are below.
- 4.13 .com – Commercial;
- 4.14 .co.uk – United Kingdom based address;
- 4.15 .org – Non profit organisation;

4.16 .gov – Government;

4.17 .nhs.uk – NHS sites;

4.18 .int – International;

4.19 .mil – Military;

4.20 **Purchasing on the Internet**

4.21 When buying goods from UK suppliers it is always important to know that your payment transactions are secure. When using Internet to purchase goods or services the image should appear when entering your payment details.



4.22 The security lock logo above shows that you have entered a secure area (SSL = Secure Server) and means entering private information is safe. If this doesn't happen, email the suppliers in question and ask what security measures they use for payment details (credit/debit cards).

Note The Trust does not allow its staff to use the Internet for personal purchase matters.

5 **EMAIL FILTERING RULES**

5.1 To help ensure that the Trust email system is protected against virus, spyware, adware, malicious software attacks and is closed to offensive material and in line with Trust policies, incoming/outgoing emails are filtered as detailed below:

- All incoming/outgoing email is monitored without interception and only those that meet any of the condition rules may be delayed.
- In the event where an email meets a rule condition and is 'quarantined' then the system automatically sends an email to the intended recipient alerting them to this fact and also provides the opportunity for the intended recipient to raise a Helpdesk call if the quarantined email has been blocked erroneously.
- Emails which have been quarantined will be retained for 3 months before being automatically deleted by the system.
- The following rules are currently implemented:
- **Blacklisted** - This rule has a list of domain names which are 'Blacklisted', thus any emails arriving from these domain names will be quarantined.

-
- **Loop Detection** - This rule will tag each email with a unique identifier to make sure that no emails are looping. Looping sometimes occurs when auto forward rules are set up. Looping can cause the email system to fail completely. Potential looping emails are quarantined.
 - **Illegal MIME format** - This rule checks to see if the email is non RFC standards compliant, and/or an invalid format that has failed DeMIME within an attachment. This is a technical requirement and is included here for the sake of completeness. Emails that meet his rule are quarantined.
 - **VBS Scripts** - This rule checks for VBScript files and SHS/SHB scrap objects. If these are detected then they are removed from the email. The stripped email is then passed to the intended recipient. **Note:** VBS means Visual Basic Scripts which is a computer language.
 - **Virus, Spyware, Adware Scanning** - This rule uses Sophos Anti-Virus software to determine the presence of a virus within an email. Any email or attachment meeting this condition is quarantined.
 - **Executables** - This rule checks for exe files. Any of the following file types will be quarantined as they are potentially dangerous and can compromise the normal operation of the system: - Batch files, Executables files, HTML applications, Java Class files, Jscript files, Netware loadable module, SHS/SHB scrap objects, VBS Script files, WSH/WSF window script files. Any email meeting this rule will be quarantined.
 - **Anti Spam Agent** - This rule checks for Spam type emails using a daily downloaded list of known Spammers. This daily list is provided automatically by the system supplier. The following categories are included:- Adult, Chain letters, Computing and Internet, Dating and Personals, Entertainment, Finance & home business, Gambling, Games and Interactive, Health and Medicine, Hoax and Rumour, Humour, Illegal material, Novelty Software, Offensive, Other, Products and services, special events. All emails meeting this rule will be quarantined.
 - **Advertisement Emails** - This rule checks for 'Adv*' near a subject and will place in the quarantined area.
 - **Spam Misspelling Dictionary** - This rule checks the Spam misspelling dictionary (l1ke th1s) and allocates a score for every entry of a Spam misspelling. If a threshold is reached then the email is quarantined.
 - **Spam Dictionary** - This rule checks the Spam dictionary.

-
- **Adult Dictionary** - This rule checks the adult dictionary.
 - **Gambling Dictionary** - This rule checks the gambling dictionary.
 - **HTML Stripper** - This rule checks for HTML active components and quarantines them if present. The stripped email is passed to the intended recipient.
 - **Offensive or Derogatory** - This rule checks the Offensive/Hate speech dictionary. All email in this category is quarantined
 - **File Size** - This rule checks the size of the message and if it exceeds 20MB then it is quarantined. Messages of this size can affect the performance of the email system.
 - **Number of recipients** - This rule checks the number of recipients an email is sent to and if the number of recipients exceeds 200 then it is quarantined. Messages of this size and type can seriously affect email system performance

6 INTERNET FILTERING RULES

- 6.1 As with the email filtering rules there are Internet filtering rules which restrict access to predefined internet sites for reasons of security, offensive material and adherence to Trust policies.
- 6.2 If an Internet site is filtered/blocked then an 'Access Denied ' page is displayed and an automatic email alert is produced detailing which site and which user has attempted to access the site.
- 6.3 The list below summarises categories of Internet sites that access is denied to:
 - Adult/ Sexually Explicit sites
 - Hate Speech, Criminal Skills, Violence, Weapons, Gambling, Hacking and remote proxies sites
 - Chat, Web based email system sites etc
 - Media and music down loads
 - Social networking sites

7 GLOSSARY

Spam – Unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Sexually explicit unsolicited e-mail is called "porn spam." Also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

HTML - (Hypertext Markup Language) - The coded format language used for creating hypertext documents on the World Wide Web and controlling how Web pages appear.

Spoofing - Email spoofing is the act of forging the header information on an email so that it appears to have originated from somewhere other than its true source. This can be done by viruses as well as by an individual to gain confidential information.