Cyber Code of Conduct

Document Control:

For Use In:	Norfolk and Norwich University Hospitals NHS Foundation Trust		
Search Keywords	Authorised Use, File Downloads, Emails specific, Email Acceptable Use, Confidentiality		
Document Author:	Head of Information Governance & Information security Manager **Supported by:** Edward Prosser-Snelling, Chief Digital Information Officer and Senior Information Risk owner.		
Document Owner:	Digital Health		
Approved By:	Caldicott and Information Governance Assurance Committee		
Ratified By:	Digital Transformation Committee		
Approval Date:	21/11/2023	**Date to be reviewed by:** This document remains current after this date but will be under review	20/11/2026
Implementation Date:	As per approval date		
Reference Number:	982		

Version History:

Version	Date	Author	Reason/Change
V11.4	November 2019	Vimmi Lutchmeah-Beeharry	Microsoft Teams usage section
V12	July 2021	Vimmi Lutchmeah-Beeharry/Ben Goss	Amended Appendix 1, 2, & 3 following DCB1596 accreditation.
V12.1	July 2023	Vimmi Lutchmeah-Beeharry/Ben Goss	1. Amended Appendix 2 to harmonise contents with the Email Charter. 2. Amended the secure domain table and referring to DCN 1579 portal
V12.2	October 2023	Vimmi Lutchmeah-Beeharry/Mike Brown	1. All email related contents have been transferred to the Microsoft Office 365 Usage Policy 2.

Previous Titles for this Document:

Previous Title/Amalgamated Titles	Date Revised
None	Not applicable

Distribution Control

Printed copies of this document should be considered out of date. The most up to date version is available from the Trust Intranet.

Consultation

The following were consulted during the development of this document:
Information Governance
Digital Health Department

Monitoring and Review of Procedural Document

The document owner is responsible for monitoring and reviewing the effectiveness of this Procedural Document. This review is continuous however as a minimum will be achieved at the point this procedural document requires a review e.g. changes in legislation, findings from incidents or document expiry.

Relationship of this document to other procedural documents

This document is a policy applicable to Norfolk and Norwich University Hospitals NHS Foundation Trust; please refer to local Trust's procedural documents for further guidance, as noted in Section 4.

Contents Page

1. Introduction

1.1. Rationale

In common with all comparable public sector organisations, Norfolk and Norwich University Hospitals NHS Foundation Trust (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 must 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 legislations, NHS Policy and UK Government standards and guidance on these matters.

The Digital Health 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.

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 related policies. The use of personal email and non-Trust authorised systems for conducting the normal business of the Trust is not permitted.

1.2. Objective

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.

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. This Code of Conduct is 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.

The primary 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.

1.3. Scope

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 Associate Director Digital Health for investigation and with potential escalation to the Local Counter Fraud Specialist NHS.

This policy also covers staff who are not employed by the Trust, but whom the Trust has granted access.

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
- Digital Health Department Responsibilities
- Good Practice Guide
- Filtering Process

1.4. Glossary

The following terms and abbreviations have been used within this document:

Term	Definition
Authorised Use	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 3.1.
Confidentiality	A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the

Term	Definition
	information will be held in confidence. It: a. is a legal obligation that is derived from case law; b. is a requirement established within professional codes of conduct; and c. must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures
Harassment	Harassment is unwanted conduct, which affects the dignity of men and women at work. This may be based on age, sex, race, religion or belief, mental or physical disability, nationality, sexual orientation, gender reassignment or some other characteristic.
Non-authorised Use	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 3.2.
Recipient	Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. Before any email is sent out, please ensure that all recipients have a legitimate right to receive and further process this data.
System Monitoring	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	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.
The Trust	Norfolk and Norwich University Hospitals NHS Foundation Trust

2. Responsibilities

2.1. Digital Health Department

The Digital Health 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.

The Digital Health Department, acting on delegated authority from the Chief Executive, is responsible for maintaining a safe and secure computing environment in the Trust.

2.2. All Staff

All staff have a responsibility to use the Trust facilities relating to all forms of electronic communication in line with this and other related Information Governance and IT Security Policies.

All staff have a responsibility to ensure that the recipient to whom data is sent has a legitimate right to receive and further process the personal information they receive in an email.

3. Policy Principles

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. 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.

This section sets out in more detail the implications of using the email and Internet system(s) for potential harassment of recipients.

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. 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. This is the case, regardless of the intention.

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.

3.1. Authorised Use

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.

Personal access to the Internet can be limited or denied by the Trust with Trust decisions being final.

3.2. File Downloads

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 Digital Health Department before a download is attempted. Further detailed guidance on this can be obtained from the IT Helpdesk.

3.3. 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 using Trust approved encryption solutions. Please contact the IT Helpdesk for further details.

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;

3.4. Email Specific

- Do not send bulk communications by email without appropriate mitigating controls and authorisation from the Information Governance Team.
- Use of Trust communications systems to set up personal businesses or send chain letters;
- Forwarding of Trust confidential messages or information to external locations;
- Ensure the recipients of an email has the legitimate right to receive and further process the information received;
- 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;

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.

3.5. Application/Systems on the Trust Infrastructure

- Developing internal Applications/Systems:
  - Requires explicit authorisation from the Senior Information Risk Owner(SIRO)
  - Is the Trust Property unless an authorised separate agreement is in place
  - Meets the Privacy by Design and Default framework and in line with the Data Protection and Confidentiality Policy
    - Completing a Data Protection Impact Assessment where necessary to identify and privacy risks.
  - Meets the requirements outlined in the Software Development Policy

- Implementing/Maintaining internal Applications/Systems:
  - All updates should be authorised by the Change Programme Board and
    - Are done without prolonged interruption/delays
    - Does not cause any data loss or corrupt data
  - Maintaining, and testing are in adherence to Trust policies and procedures covering the operation of the business;
  - Business Continuity is in place for such applications/Systems and has been tested.

3.6. Confidentiality

Users are bound by the terms of the Trust's Data Protection and Confidentiality Policy (Trust Docs ID: 718)

Under the Data Protection Act 2018 users must ensure that they only disclose information relating to an identifiable individual if there is a legal basis to do so. Additionally, they may not disclose confidential information relating to any aspect of the business of the NHS unless they have authority to do so. A summary of the main provisions of the Data Protection Act 2018 is available on Trust Docs ID: 13696

The following should be taken into account when using email to send confidential information:

- Users should ensure that senders and recipients should understand the risks of using email as a communication channel and agree what will and will not be sent.
- Where email messages do contain confidential information they should be clearly marked 'Confidential' and comply with the email acceptable use policy (Appendix 1) and the sending person confidential data using email guidance.

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.

3.7. Monitoring

It is essential an employer has clear policies and guidelines in place to monitor the use of email, the internet and other forms of electronic transmissions.

The Trust has charged the Digital Health 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. 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

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 Cyber Code of Conduct will be notified to users and the latest updated copy of the Cyber Code of Conduct will be made available via the Trust's Intranet.

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.

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.

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.

In cases of suspected abuse or unauthorised use of email, internet or other electronic communication systems, the Trust may instigate an investigation that

could lead to formal disciplinary action or criminal proceedings being taken against an individual(s).Freedom of Information
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.

3.8. Counter Fraud

Users are bound by the terms of the Trust's Anti-fraud and Bribery Policy (Trust Docs ID: 7428)

All employees have a personal responsibility to protect the assets of the Trust, including all buildings, equipment and monies from fraud, theft, corruption or any other irregularity.

3.9. Use of the Trust Name

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.

3.10. Intellectual Property

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.

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.

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.

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.

3.11. Legal Matters

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' should be used in emails in the same way as on letters or faxes.

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.

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.

It is not permissible to offer a prospective applicant employment via email.
If users have concerns over the legal status of an intended message they should discuss their concerns with their immediate manager.

3.12. User Registration

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.

All users are contractually bound by this and other Trust policies and any changes that may be made to them from time to time.

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.

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.

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.

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.

Users are not permitted without express permission of the Digital Health Department to create their own Internet or Intranet sites on any part of the Trust IT infrastructure.

4. Related Documents

- Anti-fraud and Bribery Policy – Trust Docs ID: 7428
- Data Protection and Confidentiality Policy – Trust Docs ID: 718
- Microsoft Office 365 Usage Policy – Trust Docs ID: 22981
- Misconduct Policy – Trust Docs ID: 15355
- Guidance for Transferring Personal Information – Trust Docs ID: 740
- Information Governance Policy – Trust Docs ID: 725

- Information Investigation Policy – Trust Docs ID: 11010
- Information Risk Policy – Trust Docs ID: 729
- IT Security Policy – Trust Docs ID: 985
- Policy for Managing Information Governance, Information / Cyber Security Related Incidents – Trust Docs ID: 10008
- Incident Management and Investigation Policy – Trust Docs ID: 15736
- Social Media Policy – Trust Docs ID: 1003
- System Level Security Policy – Trust Docs ID: 751
- Security and Confidentiality of Patient and Personal Information – Trust Docs ID: 738
- Data Protection 2018 Principles – Trust Docs ID: 13696
- Software Development Policy – Trust Docs ID:19225.

5. References

- NHS Employers
- UK General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Fraud Act 2006 (legislation.gov.uk)
- Bribery Act 2010

6. Monitoring Compliance

Compliance with the process will be monitored through the following:

Key elements	Process for Monitoring	By Whom (Individual / group /committee)	Responsible Governance Committee /dept	Frequency of monitoring
Monitoring activity	Review	Digital Health	Digital Health	Annual

The audit results are to be discussed at relevant governance meetings to review the results and recommendations for further action. Then sent to Caldicott and Information Governance Assurance Committee who will ensure that the actions and recommendations are suitable and sufficient.

7. Equality Impact Assessment (EIA)

Type of function or policy	Existing

Division	Corporate	**Department**	Information Governance/Digital Health
Name of person completing form	Gemma Lynch on behalf of Vimmi Lutchmeah-Beeharry	**Date**	July 2023

Equality Area	**Potential** **Negative Impact**	**Impact** **Positive Impact**	**Which groups are affected**	**Full Impact Assessment Required YES/NO**
Race	No	No	n/a	No
Pregnancy & Maternity	No	No	n/a	No
Disability	No	No	n/a	No
Religion and beliefs	No	No	n/a	No
Sex	No	No	n/a	No
Gender reassignment	No	No	n/a	No
Sexual Orientation	No	No	n/a	No
Age	No	No	n/a	No
Marriage & Civil Partnership	No	No	n/a	No
EDS2 – How does this change impact the Equality and Diversity Strategic plan (contact HR or see EDS2 plan)?				

- **A full assessment will only be required if: The impact is potentially discriminatory under the general equality duty**
- **Any groups of patients/staff/visitors or communities could be potentially disadvantaged by the policy or function/service**
- **The policy or function/service is assessed to be of high significance**

IF IN DOUBT A FULL IMPACT ASSESSMENT FORM IS REQUIRED

The review of the existing policy re-affirms the rights of all groups and clarifies the individual, managerial and organisational responsibilities in line with statutory and best practice guidance.

Appendix 1: Email and Internet Acceptable Use Policy

8. Introduction

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 in compliance with its own policies and current legislation this acceptable use policy to guide best operating practice.

Most users of the Internet are unaware of the potential implications and risks (potential harassment, discrimination and employers being compromised by staff etc.)

The Trust is accredited with NHS Digital against the DCB1596 Secure Mail Standard, this means that the Trust has put in place and evidenced a number of safeguards around its e-mail environments to allow for the secure transfer of e-mail.

9. Purpose

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 could 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;
- Loss of efficiency

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.

10. Good Email Practice

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’ts of use and is not intended to be exhaustive.

Security

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.

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

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.

Junk email also known as spam and chain letters can also contain viruses so don't open them or send them on – delete them.

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 Network & Security Manager for analysis and investigation prior to being deleted. If appropriate, relevant emails may subsequently be forwarded to the Local Counter Fraud Specialist.

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.

Confidentiality

The identity of an e-mail sender can be faked which is known as spoofing. If you receive an apparently legitimate e-mail 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 e-mail system. If in doubt, refer any suspicious e-mails to the Trust's Digital Health Security Team to undertake further enquiries to validate any request. Where appropriate, relevant e-mails may be forwarded to the Local Counter Fraud Specialist for investigation.

Confidential information can be anything which relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored and can include: patient data; professional and contract performance data; information around HR, payroll, salaries and occupational health; sensitive requests, complaints, investigations, papers for meeting which contain confidential subject matter, Serious Case Reviews, and Serious Untoward Incidents.

E-mails containing personal identifiable or special category (sensitive) information must be stored appropriately on receipt, e.g. incorporated within the health record and deleted from the e-mail system when no longer needed.

Use appropriate and authorised methods to send special category (sensitive) patient data to other organisations. Using unencrypted e-mail to other non-NHS organisations is not a secure means of communication and could result in the e-mail being intercepted.

Check the content of the data being sent, including the body of any e-mail, all attachments and the recipient list when replying to an e-mail as there could be someone who is not authorised to receive it.

When sending an e-mail to a network distribution list, you should check the distribution list membership prior to sending the e-mail to ensure the membership is appropriate.

Ensure sensitive internal documents are always marked with an appropriate phrase like ‘For Internal use only‘. If sensitive documents are not marked with appropriate phrase, the recipient could unknowingly pass on confidential information without being aware.

Never use a person’s full name as the subject heading of an e-mail.

Legal

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.

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.

Any discussion, views or quotes using the Trust email system could lead to a lawsuit which can be potentially very damaging.

Only send what you have the legal right to pass on. Sending unidentified copyright material could lead to legal action.

Etiquette

Use upper and lower case letter as in a normal sentence. Don’t use all caps as this is considered shouting. The use of email disclaimers is recognised as good practice, though not legally binding. The following format should be used in Arial, 12pt, black type:

Name	
Job Title	
Tel:	XXXXXX
Mobile:	if you have a work mobile number
Email:	name.surname@nnuh.nhs.uk
Trust Name	Norfolk and Norwich University Hospitals NHS Foundation Trust
Website:	http://www.nnuh.nhs.uk/
SPACE	
[Address of onsite work location]	

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.

Email Filtering Rules

Cyber Code of Conduct

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 or emails addresses which are ‘Blacklisted‘, thus any emails arriving from these domain names or emails addresses 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.
- **Virus, Spyware, Adware Scanning -** This rule uses scanning 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 Policy -** 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.
- **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 30MB 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.

11. Good Internet Practice

This section sets out a guide to the best industry practice in the efficient and proper use of the Internet.

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.

If an Internet site is filtered/blocked then an 'Access Denied 'page is displayed.

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 downloads
- Social networking sites

12. Appendix 2 – Digital Health Department

User Name	
Title	
Ward / Department	
Telephone Number	
Line Manager	
Division / Directorate	

Users Declaration

I UNDERSTAND THAT:

Cyber Code of Conduct

- I must **not,** under any circumstances, allow anyone knowledge of my password.

- If it does become known **I will** immediately instigate a password change to ensure that system security is maintained.

- I accept that if I fail to protect my password my access will be terminated immediately.

- I have read a copy of the Trust Cyber Code of Conduct and agree to abide it.

Signed: --

(User's signature)

Trust Managers / Supervisor's Authorisation: ---

Once complete please place in the user's personal file.