University Hospitals of Leicester NHS
NHS Trust

Email and Internet Usage Policy

Approved By:	Policy and Guideline Committee
Date of Original Approval:	9th October 2003 – Trust Board
Trust Reference:	B26/2024 (formerly A9/2003 – categorisation changed at the 11 April 2024 Trust Board. Audit Committee is now the approving body for this policy)
Version:	3
Supersedes:	2 – November 2020
Trust Lead:	Saiful Choudhury, Head of Privacy
Board Director Lead:	Andrew Carruthers, Chief Information Officer & Senior Information Risk Owner
Date of Latest Approval	24 June 2024 – Audit Committee
Next Review Date:	June 2027

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

Version No	*Amendments Made*	*Authorisation*
2	This policy has been re written to incorporate Data Protection Act 2018 and GDPR 2016 incorporated where applicable and also to incorporate email retention processes	Privacy Unit
3	Change to policy -50Gb rather than 10Gb or 12 months retention whichever comes first. Users are responsible for deleting items that have been read and not required. Removal of Appendix F as this was no longer required.	Privacy unit

KEY WORDS

Email, Internet, Encryption, nhs.net, Spam, Phishing

1 INTRODUCTION AND OVERVIEW

1.1 This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures for Email and Internet Usage within the Trust, including usage outside of the Trust premises using devices that have been approved by the Trust.

1.2 This policy covers the use of services in relation to the internet, Trust email accounts and NHS email accounts. The policy similarly establishes employee responsibility in the use of these. In implementing this policy, the Trust aims to maximise the benefits of internet and email access whilst minimising potential risks.

1.3 The NHS has a national private network (HSCN), which, as well as having its own private information bases, also acts as a gateway for accessing the internet. For the purposes of this policy, the term “internet” will be used as a generic description of internet and HSCN services. The internet is an extremely useful information tool but it is one with inherent security risks and without guarantees of reliability or performance.

1.4 The wide range of information available on the Internet and the nature of the Internet and Email raises concerns about security, confidentiality and proper conduct. This document contains the policy statements to which Trust employees must abide in order to protect patients, as well as Trust staff.

1.5 The objectives of this policy are to:

- Identify proper use of the internet and email in support of the organisation’s task;
- Ensure employees are aware of proper conduct when using the internet and email;
- Ensure that all employees are responsible, productive internet and email users and that they are protecting the Trust’s public image.
- Ensure that all the Trust is Cyber Security protected, and that all employees are made aware on how to maintain this

2 POLICY SCOPE

2.1 This policy applies to all members of staff employed by UHL, that use email and internet. It also applies to honorary contract holders, secondees, locum staff, bank staff, voluntary workers and agency staff using the resources of the Trust, as well as contractors.

2.2 Managers at all levels are responsible for ensuring that their staff are aware of and adhere to this policy.

2.3 This policy will apply to access to Trust Email accounts and Internet usage that relate to Trust business use only and should not be used for any personal use without prior authorization from line management.

3 DEFINITIONS AND ABBREVIATIONS

3.1 The following terms and acronyms are used within the document:

- **IM&T** - Information Management & Technology
- **IT** - Information Technology
- **HSCN** - NHS national private network
- **NHS** - National Health Service
- **NHSmail** - The NHS web-based mail service (NHS.net)
- **PC** - Personal Computer
- **WWW** - World Wide Web
- **Phishing**- a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data.
- **Spam**- any unwanted, unsolicited digital communication, often an email, that gets sent out in bulk
- **Cloud Storage**- a model of computer data storage in which digital data is stored in logical pools, said to be on 'the cloud'.
- **Virtual Desktop Info structure (VDI)** allows users to connect to the trust network and resources securely over public network via personal devices (internet)
- **Virtual Private Network (VPN)** allows users to connect to the trust network and resources securely over the public network via trust devices (internet)

4 Roles and Responsibilities

4.1 **Chief Information Officer- Senior Information Risk Officer (SIRO):** The trust Senior Information Risk Owner (SIRO) is the Executive Director Lead for this policy. The key responsibilities of the SIRO for this policy are:

- To review the implementation of this policy.
- To determine actions for breaches of this policy with Head of Privacy,

4.2 **Head of Privacy- Data Protection Officer:** The Trust's Head of Privacy has responsibility for managing the overall co-ordination, publicising and monitoring of the Trust IG Framework.

The Trust's IG Lead Head of Privacy has specific responsibility for;

- The development of the IG strategy and procedure and guidance related to this policy

- Leading training and audit strategies to raise IG standards and services within this policy
- Ensuring compliance with Legal requirements

4.3 Department Managers

Are responisble for working with their employees to support implementation of policy requirements.

Are responsible for the identification of staff training requirements and for making arrangements for addressing staff training requirements through individual personal development plans.

Are responsible for ensuring that their staff are aware of the Email and Internet Usage Policy guidance, its requirements and implementation.

Should review the usage of the Internet access made by their staff, to ensure that staff access to the Internet facilities does not interfere with Trust business, if managers suspect innapropriate usage. Where managers have concerns about staff internet use they are to contact the Privacy Unit for advice. HR input will be required and reporting will be conducted via IT Service Desk. See Appendix D for more information.

Where staff have concerns about the records relating to their own access they can request usage reports via the IT Service Desk.

4.4 Employees & staff working on behalf of the Trust

All Trust employees, whether permanent, temporary or contracted, and students and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. This policy requires all staff to understand the need;

- To comply with all information standards;
- To hold information securely and confidentially;
- To obtain information fairly and efficiently;
- To record information accurately and reliably;
- To share information appropriately and lawfully

5. POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS

5.1 Internet

5.1.1 The Trust will take all reasonable steps to ensure that users of the Internet service are aware of policies, protocols, procedures and legal obligations relating to the use of Email and the Internet. This will be done through training and staff communications at departmental and organisation-wide levels.

5.1.2 The Organisation will ensure all users of the Email and Internet facilities are registered and that access is linked to agreed levels of authority.

5.1.3 Under no circumstances will patients and visitors be given access to Trust data and systems including access to Internet and Email facilities using Trust

equipment. Unless it is to fulfill legal and legislative purposes. Please refer to the Control of Access to Electronic Systems Policy B25/2007 for further guidance.

5.1.4 Staff who do not use a computer for their work may have access to a designated computer in their department or location at the discretion of their line manager. Staff must not access or distribute any material which is (or participate in any chatroom or Internet community whose subject matter is) unlawful, or causing of offence, examples of which are material which is libellous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability. This also includes incitement of hatred and violence or any activity that contravenes the Trust's Policies including Equality and Inclusion Policy B61/2011. This requirement applies even if a specific site is not blocked by the Trust access control software.

5.1.5 Access to Internet sites will be controlled by content management software which blocks access to sites considered inappropriate.

5.1.6 Access to categories of sites that are not considered to be business related will be permitted, but this is not an entitlement and should not impact normal daily work. Managers will be actively monitoring usage and will take appropriate action in the event of excessive use. In particular, users should not post work related comments on to social media sites unless it is for trust use only on approved trust page. For a list of these please liaise with the Communications Team. Further guidance is set out in the Social Networking Media Guidelines.

5.1.7 If an employee accidentally accesses material which they feel may be considered of an offensive nature, they may wish to note the time and web site address, exit from the site and then inform their line manager.

5.1.8 If an employee is in doubt about whether it is appropriate for them to access a site, they should obtain the approval of their line manager before doing so.

5.1.9 Internet users must be aware that the Internet is inherently insecure and confidential information in relation to the business of the Trust and/or person-identifiable information must never be disclosed. Although the Trust has anti-virus defences in place, great care should be taken when using the Internet. The IT Service Desk (ext. 18000) should be informed if any suspicion of virus infection arises.

5.1.10 Downloading or distribution of copyrighted material without permission of the copyright holder, or of software for which the user does not have a legitimate licence is forbidden, this applies equally to downloads for work or personal use.

5.1.11 Access to media streaming sites, will be blocked unless it is required for business purposes. Streaming media uses significant network bandwidth and can affect the performance of business applications, including clinical systems. Users can request access to media streaming sites for stated business purposes for a specified period of time, with their line manager's approval, through the IT Service Desk.

5.1.12 Access to cloud storage sites, such as Dropbox and SkyDrive will be blocked to prevent data loss. Where colleagues wish to store outside of the Trust PC hard disc which may have limited physical space – the trust supports cloud storage as a solution – the approved one is currently Sharepoint Online and Onedrive. Use of this or other cloud storage sites should be put through to IT Service desk for consideration.

5.2 For clarity

E-mail and internet are an integral part of communication throughout the Trust.

Trust staff are not authorised to load any software onto any Trust computer system without the permission of the IT Department and any attempt to install software is strictly prohibited. If there is a particular one-off requirement to do this, employees should liaise with the IT Service Desk, who will assist with any further precautions, which may be necessary. If this advice is not followed, employees will be personally responsible for any loss of data of their own systems.

5.3 Email

5.3.1 Access under the Regulation and Investigatory Powers Act 2000 which would require Chief Executive approval and would be used in circumstances where for example a crime was suspected.

- As part of an automated process to allow encryption to take place i.e. non-human intervention
- In response to a request under the Data Protection Act, Freedom of Information Act and potential Access to Health Records Act.
- In circumstances were the individual was on long term sick or unavailable and business continuity arrangements required access - this would be approved by a line manager for access by a nominated individual.

5.3.2 Access to emails is via Outlook Online in a web browser.

5.3.3 Microsoft Outlook has the option to allow another person, known as a delegate to receive and respond to e-mail messages and meeting requests and responses on their behalf. The person granting delegate permission determines the folders the delegate can access and the changes the delegate can make. Additional permissions may be granted that allow the delegate to read, create, or have more control over items in the mailbox.

5.3.4 In exceptional circumstances, e.g. unexpected long-term absence, the IT Department may grant permission for a Line Manager to have delegate access to the employees mailbox.

5.3.5 If an employee gives delegate access to another employee, this may allow them to access personal and sensitive information inappropriately. The employee who granted the access will be held responsible for any use of this information.

5.3.6 Any Email sent or received by an employee is deemed to be Trust property and as such is subject to the Trust's Records Management policies and procedures. Unless marked Personal in the 'Subject Field' Email may be opened by the Trust. It must be noted, however, that any Email marked 'Personal' may be opened in such circumstances that include (but not limited to): staff absence and named person/line manager is looking after mailbox. If the person has left and emails need to be reviewed while transition arrangements to remove the email account takes place.

5.4 Staff must not distribute any material which is unlawful, or causing of offence, examples of which are material which is libelous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political

convictions, or disability. This also includes incitement to commit a crime, incitement of hatred and violence or any activity that contravenes any of the Trust's policies including Equality and Inclusion Policy B61/2011. This also includes material that could be classed as abusive, indecent, obscene, menacing; or in breach of confidence, copyright, privacy or any other rights. Distribution of such material may result in legal action in addition to Trust disciplinary procedures. The Trust reserves the right to monitor all Email and is required to do so under law according to Principle F of GDPR (2018).

Staff must not initiate or forward electronic chain letters, forge or anonymously send Email or make any attempt to infect other systems with computer viruses. If staff receive such Email and have concerns over the content, they should contact the IT Service Desk (ext 8000) and forward the email to Phishing@uhl-tr.nhs.uk.

Staff who receive Email attachments which they have any doubts about the origin and/or content of should contact the IT Service Desk for advice.

Under no circumstances is patient identifiable data or sensitive information to be sent over the Internet in an unencrypted form. See Appendix E for more information.

5.5 Where there is apparent cause for concern at an employee's use of the email facility the agreed process will be pursued which shall include the obtaining of records through the IM&T Department. See Appendix D of this document.

5.6 Personal email accounts and 3rd party messaging (such as Hotmail,Doctors.net and WhatsApp) are insecure and must not be used to transmit or receive Patient Confidential data, or any email that contained Personal identifiable data or any data that could identify an individual. Sensitive or patient-identifiable information must not be forwarded to University accounts.

5.7 Trust email can be accessed remotely on any client via the Microsoft Online (m365) platform in a browser on a PC or the Microsoft Outlook App on a mobile device. Provided the user is registered with Multi Factor Authentification to access their trust email.

5.8 E-mail and web site publishing have the same legal status as written documents; therefore staff must take care to ensure that facilities are used legally and avoid (for example) defamation, breach of copyright, breach of confidence etc. Staff must also write e-mails in the same courteous manner as letters and documents which are printed. Staff must also be aware that any or all e-mails can be required as evidence in a court of law.

5.9 Trust facilities must not be used in a way which would breach the Computer Misuse Act 1990, for example, hacking (such as logging onto another employee's email account), virus transmission or unauthorised access to systems.

5.10 Staff must not transmit or intentionally access any material which is (or participate in any social chatroom or internet community whose subject matter is) unlawful or which is or could reasonably be deemed to be, objectionable or likely to cause offence to the public at large.

5.11 Staff must be aware that whilst the immediate recipient may not find a

transmission to be offensive or objectionable the transmission may well be forwarded to a wider audience which may do so.

5.12 The Trust will restrict access to the type of site mentioned above, and to other sites deemed unsuitable such as social networking sites so as to prevent accidental access.

5.13 Users must not download, distribute or install software not supported by the Trusts IM&T Department. Any queries should be referred to the IM&T Service Desk on ext 18000.

5.14 Staff are responsible for managing their own personal mailboxes (and any departmental multi-user email inboxes they have access to) in accordance with the Trust's Policy for the Retention of Records (Trust reference B10/2004). Emails that contain patient care details, key business decisions etc. must not be 1) deleted or 2) remain in personal mailboxes (the entire mailbox and account will be deleted after an individual leaves the Trust). Arrangements must be made for that information to be saved to an appropriate electronic system, network drive or printed and stored in a relevant paper record.

5.15 Email accounts and Inbox folders in your Email system MUST NOT be used to store information, this should be saved within the Trust normal network file structures.

5.16 Staff must be aware that all e-mails are potentially subject to disclosure under the Freedom of Information Act or the Data Protection legislation and to modify their content and language as appropriate for a professional environment.

5.17 The Trust may forward details of e-mail account holders to the appropriate body for Inclusion in the national (NHS) e-mail system (NHS Mail).

5.18 The Trust restricts e-mail messages to 35Mb.

The Trust will impose quotas on user's mailbox sizes. See Appendix C for further details. Use up to 50gb or 12 month retention (whichever comes first) – Colleagues are requested to ensure they make their own provision on the shared drive for any emails they deem valuable to retain.

Line managers should support department wide provisions in terms of where staff should be keeping emails pertaining to the department.

6 WHAT IS APPROPRIATE EMPLOYEE INTERNET USAGE

6.1 Employees must exercise good judgement and remain productive at work while using the internet.

6.2 Employees may not use UHL's Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or

inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.

6.3 Disparaging, abusive, profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail—are forbidden.

6.4 Copyrighted materials belonging to entities other than UHL may not be transmitted by employees on the company's network without permission of the copyright holder.

6.5 Employees may not use UHL's computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files (unless it is a legitimate requirement of process and no other alternative method of dissemeniation is available) and spamming (sending unsolicited e-mail to thousands of users).

6.6 Employees are prohibited from downloading software or other program files or online services from the Internet without prior approval from the IT department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into company systems and networks.

6.7 Every employee of UHL is responsible for the content of all text, audio, video or image files that he or she places or sends over the company's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. UHL's corporate identity is attached to all outgoing e-mail communications, which should reflect corporate values and appropriate workplace language and conduct.

7 EDUCATION AND TRAINING REQUIREMENTS

7.1 Reading this policy is a requirement of local induction.

7.2 Use of e-mail and the internet is included in the Information Governance Communications Plan.

7.3 Mandatory training is undertaken via HELM. There are 3 modules-

- Cyber Security Level 1
- Cyber Security Level 2
- Information Governance

8 PROCESS FOR MONITORING COMPLIANCE

Compliance and monitoring

8.1 Monitoring and periodic auditing of usage of the internet and email are performed in order to ensure the integrity of the Trust's systems and compliance with NHS Digital Security requirements.

8.2 The software which is used to restrict access to sites also logs internet traffic. Logs will be analysed to report on the Trust's internet usage. Suspicious behaviour or what appears to be exceptionally high usage will be investigated.

8.3 Software that monitors the content of e-mails to ensure compliance with Trust policy is used at UHL and emails that contain profane or abusive language will be blocked. Users will be notified and logs of blocked emails are kept by IM&T.

POLICY MONITORING TABLE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements Who or what committee will the completed report go to.
Internet Usage	IT Department	Compliance Report, Ad Hoc Reporting	E-Communications Group, Departmental Managers	Quarterly, On Request
Email Usage	IT Department	Ad Hoc Reporting	E-Communications Group	Ad Hoc

9 EQUALITY IMPACT ASSESSMENT

9.1 The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

9.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

10 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

There following legislation/guidelines govern the transmission of electronic information and the monitoring of activity which organisations may undertake:

- The Post Office Act (1953)
- Obscene Publications Act (1959/1964)
- The Race Relations Act (1976)
- The Protection of Children Act (1978)
- Telecommunications Act (1984)
- The Criminal Justice Act (1988)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- Copyright (Designs and Patents Act, 1988) as amended by the Copyright (Computer Programs) Regulations 1992.
- Data Protection Act (2018)
- The General Data Protection Regulation (2016)
- The Regulation of Investigatory Powers Act (2000)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
- Employment Practices Data Protection Code – Part 3, Monitoring at Work (Information Commissioner)
- The Freedom of Information Act (2000)

11 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts PAGL system.

Appendix A

E-mailing patients

A1. Introduction

The Department of Health (DoH) position is quite clear on the requirement to secure patient data which is transmitted electronically.

“The movement of unencrypted person identifiable data held in electronic format should not be allowed in the NHS This includes the use of e-mail to transmit patient data within and outside of the NHS.

A2. Background

DoH guidance, Trust Policy and the Data Protection legislation requires the Trust to handle patient’s information securely. As noted above information which is transferred between NHS organisations and between the NHS and third party requires encryption. See Appendix E for more information.

However, there is a significant difference between using insecure e-mail to transfer data about a patient (over which the patient has no knowledge) and using insecure e-mail to communicate with a patient when the patient has had the opportunity to make an informed choice to use e-mail.

Patient consent to using e-mail as a communication method must be sought before patients are e-mailed See Appendix F for more information. Staff should contact patients to ensure they have recorded consent that the patient has consented for communications to be sent to them via email and it should not be assumed.

A3. Considerations before using e-mail as a communication channel

- You should consider the sensitivity of the information to be sent and if e-mail is the most appropriate communication method.
- E-mail is an informal communication method. Is the information going to be less clear and open to misinterpretation than if the information was sent by letter?
- The Trust e-mail system and NHSMail are not suitable for holding medical records, therefore clinical information must be held in the patient notes or as part of an existing electronic system. New repositories of patient information must not be created for holding e-mails which have been sent to patients.
- To use e-mail the patient must be over 16 years of age and have capacity.
- The patient must be informed that e-mail is not secure (see A5) and the patient must consent to having understood the risk.
- Information about a patient must not be sent via insecure e-mail to a relative or carer without the consent of the patient (unless the relative or carer is a legally designated decision maker).
- Services should be provided through a shared mailbox to which a number of people have access to ensure continuity when staff leave, sickness etc.

A4. Responsibility

Responsibility for adherence to this policy and with the management and use of shared mailboxes lies within IM&T department in conjunction with the Privacy Unit.

A5. Security of e-mail

This advice is posted on the Trusts web site (under Terms and Conditions section 7). Patients should be made aware that e-mail is insecure before the Trust agrees to send confidential data via e-mail. See Appendix F for more information.

The security of e-mail

There are a number of potential risks when using e-mail of which users should be aware. This is a non-technical (and very simplified) explanation of some of the confidentiality risks which exist.

Issues with e-mail
When you send an e-mail message, the message is sent in clear text, so anyone can read the content.

It is unlikely that the message you send will go straight to the computer from where it will be read. The message will be sent to a computer nearer to its final destination like a sequence of post boxes. Each time the e-mail goes through a post box, a copy remains in the post box. Because of the way the internet works, it is impossible to know how many post boxes the e-mail will go through on its journey. See figure 1.

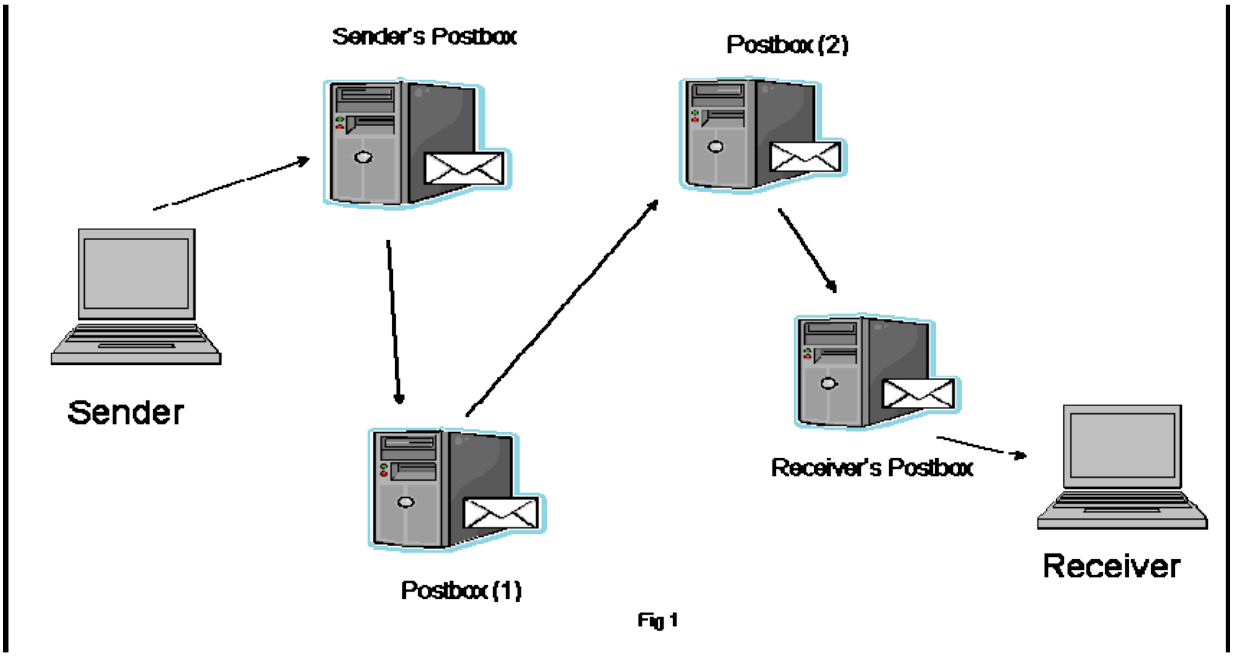


Fig 1

In figure 1, the message remains in post boxes (1) and (2) until the owners of those post boxes delete the message, even if the sender and receiver delete the message. So anyone who gains

access to the post box has access to your e-mail message.

A.6 There are many risks with emails:

- E-mail may be sent to the wrong address by any sender or receiver;
- E-mail is easier to forge than handwritten or signed papers;
- E-mail can be intercepted, altered, forwarded, or used without detection or authorisation;
- E-mail delivery is not guaranteed.

These are potential problems of which you should be aware, however, e-mail is convenient and used by millions of people every day.

Advice to staff and patients

- E-mail has been likened to sending a post card. Our advice is do not put anything in an e-mail if you are concerned about someone else seeing it.

- There is no guarantee of delivery, or delivery time, when using e-mail so do not use it in cases of emergency.

- It is your responsibility to follow up with the Trust if you have not received a response to your e-mail within a reasonable period of time.

- If you have asked the Trust to communicate with you via e-mail it is your responsibility to advise the Trust of any change of e-mail address. You may withdraw your consent for the Trust to communicate with you via e-mail at any time.

- You should be aware that if you share your computer it may be possible for other people to be able to see emails you have sent or sites you have visited on the Internet, as your computer keeps a record of these.

- To protect against viruses and SPAM we ask that attachments are not included within emails to UHL, unless the recipient has arranged this and is expecting to receive one. If we suspect your email contains these, we may delete it without opening to prevent any damage to the Trust systems and services. Patients must be informed of this via reply if you are in patient/uhl staff member email dialogue.

Appendix B

Dos and Don'ts concerning the use of Email and the Internet

Do forward spam emails or 'phishing' emails to this address: Phishing@uhl-tr.nhs.uk

Do remember that emails have the same standing in law as other written communication and can be released under Freedom of Information and Data Protection legislation or to a court of law.

Do check lists carefully if using distribution lists to disseminate personal or commercially sensitive info.

Do apply common email etiquette when composing messages, e.g.

- The inappropriate use of CAPITALS is considered to be aggressive
- Standard (Arial or Times New Roman) fonts in an appropriate size should be used.
- Excessive use of acronyms and mobile phone "text speak" should be avoided.
- Care should be taken with content. Nothing should be written in an Email that would not be written in a letter or said to someone face to face.
- The same conventions should be used as when sending a letter by post, e.g. using the same style of greeting.

Do remember that the Internet is, to a great extent, uncontrolled and so information held on it must be treated with care and not automatically accepted as accurate and/or correct.

Do take great care when entering personal details on websites. There is no guarantee that any information entered is not visible to individuals other than the expected recipient.

Do use e-mail and internet facilities for limited personal use only and **Do** read the Social Networking Guidelines (B26/2010).

Do use the BCC (blind copy) facility if you do not want all recipients on a distribution list to know who else has received an e-mail.

Do use "out of office replies" (which will be sent to the rest of the trust and organisations outside of the Leicestershire Health Community if required).

Do send personal and confidential information safely.

Don't initiate or forward "spam" emails. Delete e-mails you consider "suspicious".

Don't attempt to download and install software from the Internet onto Trust computing equipment such as Trust iPads and Trust mobile phones.

Don't send or forward emails which may be reasonably deemed to be objectionable or likely to cause offence to the public at large.

Appendix C Best practice in using e-mail efficiently

An ‘online’ Archive facility can be provisioned in m365 on request. This can be applied for through LANdesk/Ivanti or a call to the IM&T team on x8000 via Line Manager.

Appendix D Manager guidance on monitoring staff computer use

D1. Introduction

This guidance is intended for use by computer systems managers who have the ability to produce audit trails of staff computer activity. This would normally be carried out as a result of routine audit reports or as a request for information on staff system usage, usually when concerns arise over the appropriateness of employee's use of the computer system.

This guideline stating the principles to apply will be applicable to systems managers who may be asked to report on the activity of staff members.

In summary, the position is:

- The Trust cannot conduct **surveillance** of staff unless sanctioned by an external body such as the Counter Fraud Service. This guideline does not consider surveillance;
- The Trust is entitled to, and does, examine it's records to satisfy itself that Trust policies are being adhered to;
- Staff should be aware that this is the case.

D2. Guideline statements

1. Systems managers are able to request internet stats from IM&T as part of investigations if they suspect "abnormal activity", this may include excessive and unusual use such as outside of normal hours, repeat enquiries on the same person and excessive failed login in attempts.and this may result in temporary suspension of the account until the investigation is complete.

2. If at any point it is considered that disciplinary action may arise, Human Resources must be informed.

3. A record of any investigatory activity should be kept. Documentation supporting the investigation should be held securely on the system and should be accessible only to staff with Systems Administrator access.

4. Requests for information on staff usage may be requested by management to determine if a Trust member was in breach of staff policies. The overriding concern in such requests is that staff members are treated fairly and it is a managers responsibility to ensure that this is the case. The best way to ensure that requests are "legitimate" is to only process requests received through Human Resources who are experienced in dealing with such matters in accordance with Trust Policy.

5. Documentation should be retained by systems managers for a maximum of 6 months after which it should be securely destroyed (any paper copies shredded). Any documentation which is used in a staff disciplinary will be held as part of the disciplinary process documentation.

6. Audit trail reports produced on a staff members activity would be disclosable to the staff member should the staff member request the information.

Appendix E

EMAIL ENCRYPTION

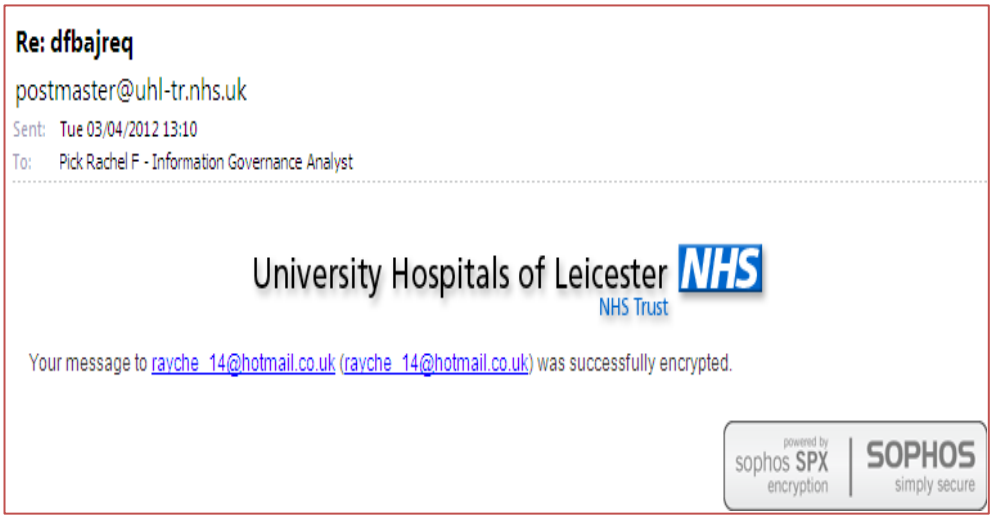
When sending confidential information outside of the Trust (and not to an already secure email address) then it is essential that you encrypt your email. This can be done automatically if you type the 2 words **UHLEncrypt** anywhere in the email.

It does not matter if the trigger phrase **UHLEncrypt** is in the beginning, middle or end of a subject title, as long as the phrase is present, it will encrypt the message. The trigger **UHLEncrypt** is not case sensitive so you can type it as: **UHLEncrypt**, **uhlencrypt**, **UHLENCRYPT**, **UhLEnCrYpt** or any other case combination, it does not matter, it will encrypt.

When you send the email externally and the trigger phrase **UHLEncrypt** is used you will receive 2 responses:

Response 1:

Response 2:



You will receive a password that will need to be communicated to the recipient by phone, without this they will not be able to view the message or open the attachments.

If you do not receive either of these messages, they MAY be in your Junk E-mail folder, so please be aware