

Network, E-Mail and Internet Acceptancy Use Policy

Version number :	9.2
Consultation Groups	
Approved by (Sponsor Group)	December 2018
Ratified by:	Information Governance Steering Group
Date ratified:	20 February 2019
Name of originator/author:	Associated Director of IT / Information Governance Steering Group
Executive Director lead :	Chief Finance Officer
Implementation Date :	February 2019
Last Review Date	September 2018
Next Review date:	February 2022

Version Control Summary

Version	Date	Author	Version	Comment/Changes
1.0	2/10/2000			Draft reviewed by Executive Team on 9 th November and for review by JSC on 15 th November. This document was intentionally brief in order to set out and agree guiding
2.0	9/11/2000			Expanded detail on operation of the policy, responsibilities and addition of an E-mail guidance and best practice section. Issued in draft to Test Users of new ELCMHT Network System
3.0	13/11/2000			Working draft with minor changes – to be presented to JSC for approval in December
3.1	31/1/2001			Minor corrections
3.2	28/2/2001			Minor corrections

3.3	17/5/2001			Adjustment to reflect new arrangements for authorising
3.4	18/8/2002			Adjustment to improve layout of service access request forms
3.5	Oct 2002			Clarification that this policy covers mobile devices
3.6	Nov 2004			Update to access request form
3.7a	Jan 05			Contents page added, Document control sheet amended, Section 3 text updated to reflect ANNEX 5, Annex 2 updated, Dormant accounts and deletion
3.7	Jan 05			ANNEX 5 added – managing e-mail accounts in accordance with Freedom of Information Act & Data
3.8	May 05			Minor changes following discussion and approval at IG Steering group (e-mail security and user responsibilities)
3.9	Aug 05			Include line manager authorisation which requires the line manager to advise the ICT Department when the user leaves the trust
4.0	Oct 05			Update Annex 1 & 2 to include the new one page easier to use request form, in line with the Registration Authority Form changes for the General update and alterations to accommodate IG toolkit requirements. Main
4.1	Nov 05			
4.2	Dec 05			Cosmetic changes following Information Governance Steering Group approval
4.3	July 2006			Working version to incorporate electronic sign on application process

4.4	Mar 2007			Additional changes to cross reference RA policy and need for credential checks on new
5.1	Dec 2007			Expansion of expected practice covering confirmed national standards for encryption and limits to use of removable devices
5.2	Jan 2008			Updated following comments and queries from users, users, additional info on NHSmail and confirmation of WinZip 11.1 and e-mail Companion
5.3	July 2008			Added information regarding Government domains that can receive encrypted e-mails
6.0	October 2008			Encryption guidelines strengthened. Guidance on 'Expected good practices on use of e-mail' and 'Managing e-mail messages' simplified, and further guidance provided. Layout of policy revised to move Standard
7.0	February 2009			Streamlined to reflect short policy and fuller procedures format following comments and queries from users.
7.1	March 2009			Deactivation of accounts altered to 6 weeks

7.2	February 2010			<p>Additional section on blogging / social networking added</p> <p>Clarification provided on using person identifiable information</p> <p>identifiable information in emails</p> <p>Instruction on obtaining a USB stick, transporting person identifiable information on USBs, and monitoring of use added</p> <p>Clarification provided on Information Security responsibilities</p> <p>Procedure for gaining access to</p>
7.3	May 2010			Instruction on USB use strengthened
7.4	March 2013			<p>Updates to entire document:</p> <p>- Removal of references to legacy</p>
9.0	March 2015			Reference to secure emailing options and
9.1	September 2015			<p>Reformatted to Trust Standard.</p> <p>Sections 3.9/3.10 now include an explanation of encrypting emails to non-secure addresses.</p> <p>New section 4.6 Generic Email addresses</p>
9.2	September 2018	Asim Mir		Review/Update

CONTENTS

1.0 Purpose of this document	4
2.0 Glossary of terms used within this document	4
3.1 Key points of this policy	7
3.2 Person identifiable or sensitive information	7
3.3 Principles and Responsibilities	8
3.4 Virus control	10
3.5 NHS Code of Connection	10
3.6 Procedure for access to internet and email services	11
3.7 Use of the Internet	12
3.8 Unintentional breaches of security	12
3.9 Use of Email	13
3.10.....	T
o send/receive between secure email services (from NHS.net to NHS.net or another secure government approved email address)	16
3.11 To send/receive between NON-secure email services (from NHS.net to an email address that is NOT a secure government approved email address)	16
3.12 To get an NHS.net account	16
4.1 Further Guidelines	18
4.2 Encryption	19
4.3 Encrypted USBMemorysticks	19
4.4 Confidentiality and Secure Storage of Data	21
4.5 Person identifiable and sensitive data:	21
4.6 Management of security	22
4.7 Generic email addresses	22
4.8 Investigation of network, email or internet use	23
4.9 Access to e-mail accounts	24

1.0 PURPOSE OF THIS DOCUMENT

1.1 This document constitutes East London NHS Foundation Trust's Internet, E-mail and Network Use Policy. The purpose of this Policy is to clearly define acceptable, permissible and safe use of the network, internet and e-mail services by the Trust's authorised users

1.2 Any reference to 'individuals' or 'users' in this Policy constitutes anyone authorised to access Trust systems including (but not exclusively) employees, volunteers, bank staff, and contractors. It also includes those who are not employed by the Trust but have authorised access to network, internet and email services through the IT equipment owned or managed by the Trust. This includes staff of third party agencies where a formal agreement to access specific Trust systems exists.

1.3 The Policy sets out:

- Relationship to other Policies
- Key points
- Definitions
- Principles and responsibilities
- Forms to be completed and declarations required from users

1.4 Relationship to other policies

This policy does not replace any other security policy within the Trust. It is intended as a guide to acceptable, permissible and safe usage within the overall Information Governance framework which includes the Information Governance and IT Security Policy, Records Management and Freedom of Information Policies of the Trust. It must be used in conjunction with these and any other relevant policy documents and procedures. It must also be used in conjunction with Trust issued best practice guidance.

2.0 GLOSSARY OF TERMS USED WITHIN THIS DOCUMENT

2.1 **Personal data** any factual information or expressions of opinion relating to an individual who can be identified directly from that information or in conjunction with any other information that is held by or comes into the possession of the data holder.

2.2 **Sensitive personal data** the eight categories of personal information defined as sensitive personal data in section 2 of the Data Protection Act 1998 (DPA) and, in this Agreement specifically including (but not limited to) information about the physical & mental health, racial or ethnic origin, sexual life or sexuality of patients or service users.

2.3 **Confidential Information** any information or combination of information that contains details about an organisation or an individual person that was provided in an expectation of confidence. This includes for example, non-personal corporate or technical information that is commercially sensitive, drafts of documents that are not ready for publication, restricted information & documents, etc. as well as personal data about patients, service users and staff.

- 2.4 **NHS Information** any information as defined in 2.1 to 2.3 above that the Data Controller owns. This includes all information supplied to the Data Processor by the Data Controller and any additional information that the Data Processor obtains during the term of the contract and shall apply equally to original NHS Information and all back-up and/or copies printed out.
- 2.5 **Data Controller** as defined in the Data Protection Act (1998) is the individual or organisation (legal person) who determines the manner and purpose of the processing personal information, including what information will be processed and how it will be obtained.
- 2.6 **Data Processor** as defined in the Data Protection Act 1998, is an individual (other than an employee of the data controller) or organisation who processes personal information whilst undertaking a business activity or service on behalf of the Data Controller, under contract.
- 2.7 **Data Processing** also defined in the Data Protection Act 1998 in respect of personal data, for the purpose of this document this includes any business activity or contracted service that involves using personal, corporate or other information including obtaining, recording, holding, viewing, storing, adapting, altering, deleting, disclosing. This is not restricted to computer processing, but includes manual files and verbal discussions.

The following definitions apply to this document:

- 2.8 **The Network** The Trust network provides individuals with access to a PC / Laptop / Mobile Device, a username, and a password protected gateway to Information, Management and Technology based services, systems and documents. Individuals must not attempt to gain access on unauthorised equipment, or without a username or password.
- 2.9 **The Internet** In the context of this policy, an Internet service means any service that can be accessed either via the public Internet, NHSnet or the Trust network and includes: Web pages, E-mail, Discussion groups and Multimedia documents, systems and databases etc. This list is not exhaustive. It includes any and all methods of information sharing or capture using any method of transmission or reception. There is no exception to this policy. The Trust reserves the right to expand this list and issue additional risk alerts and instructions to staff as and when required.
- 2.10 **E-mail** The Trust network connections enable the simultaneous connection of users to both internet and e-mail services. The usage policy principles are similar. This policy forms a single document covering both services.
- 2.11 **Mobile devices, portable and removable media** The principles and good practice of this policy apply equally to the use of removable media (including CD-ROMs, DVDs, memory sticks and portable hard drives); mobile devices such as laptops, tablets, telephones, Smartphones, pagers and air-calls and the services they provide (e.g. texting) It includes any and all methods of information sharing or

capture using any method of transmission or reception.

- 2.12 **Users** In the context of this policy, the term 'users' or 'individuals' refers equally to employees, volunteers, bank staff, and contractors. It also includes those who are not employed by the trust but have authorised access to network, internet and email services through the IT equipment owned or managed by the trust. This includes staff of third party agencies where a formal agreement to access specific trust systems exists. The contents of the policy also apply to generic accounts which are set up for use by a group of individuals.

3.1 PERSON IDENTIFIABLE OR SENSITIVE INFORMATION

Where not anonymised this must only be sent via a secure email transmission method, as below:

- From one elft.nhs.uk account to another elft.nhs.uk account
- From one nhs.net account to another nhs.net account
- From an nhs.net account to a secure government domain (as later defined)
- From an nhs.net email address to any other email address using the [secure] transfer facility

All transfers of data must respect the following:

- All network services are primarily for work related activities. Limited personal use is permitted providing it does not interfere with work performance;
- Junk mail must not be sent or forwarded;
- Use of network services may be monitored;
- Illicit, illegal or offensive material must not knowingly be requested, sent, forwarded, published or downloaded;
- Discriminatory, offensive or libellous language must not be used;
- E-mails must be concise and business like;
- E-mail boxes must be regularly checked and cleared;
- Inactive accounts will be de-activated after 90 days;
- Passwords must not be shared under any circumstances;
- PCs must not be left unattended without being logged off or locked down (ctrl/alt/delete then Lock this Computer);
- E-mails that are records must be stored in a secure network location using agreed filing and naming conventions;
- Occasionally, an individual's mailbox may be accessed by the individual's line manager, or Trust Director in response to a genuine need to do so. This access will be provided by the IT department and formally recorded;
- Individuals have a personal responsibility to use and manage e-mails and their internet usage effectively and appropriately;
- Remember that emails are just another form of trust document and are subject to Freedom of Information requests in the same way as any other trust document.

- Information security or confidentiality breaches must be reported via Datix, the Trust's incident reporting system;
- References to email, internet and network services also include the use of mobile devices including any portable media, Encrypted USBs, Smartphones, telephones, and other portable or removable devices;
- Only Trust encrypted USB sticks may be used. Individuals must not use any other sticks even if they are encrypted, to avoid the encryption being switched off;
- Current best practice guidance must be followed at all times

Failure to comply with this policy may result in disciplinary action being taken, which may result in dismissal or criminal prosecution.

PRINCIPLES AND RESPONSIBILITIES **General/Network Services**

All network services are primarily for relevant work related activities – including works council / trade union purposes. The Trust takes the final decision on what constitutes excessive or inappropriate use. Limited personal use is permitted providing it does not interfere with work performance and that individuals recognise and accept that any use of the service may be subject to audit and inspection. Personal access to the Internet can be limited or denied by a Line Manager. All individuals within the Trust must ensure that computer systems and the data accessed through those systems are safe and secure.

Username and password management

The IT Department or its nominated agents are responsible for username and password management, including:

- Setting up new users in accordance with the agreed naming convention
- Issuing passwords
- Deleting expired accounts
- Disabling dormant accounts
- Removing access rights when staff leave the Trust
- Undertaking regular audits to support these functions

Clinical systems

Additional identity and credential checking will be carried out before access to national clinical systems is granted to new users – this is covered in the Trust's 'Registration Authority Policy and Procedure'. Individuals who are authorised to access clinical systems have additional responsibilities relating to security, confidentiality and appropriate use.

Personal responsibilities

Individuals have a responsibility to ensure copyright and licensing laws are

not breached. Consequently, individuals must not download, send (or knowingly receive) software, data or images for use within the Trust unless the explicit approval of the copyright owner or licensee has been obtained.

Individuals must not knowingly request, send / forward, access, publish, download or obtain illicit or illegal or offensive material via any internet or e-mail service (this includes racist, intolerant, pornographic or sexual material and offensive comments based on an individual's gender, age, sexuality, race, disability or appearance). Receipt of such material must be reported to the IT Service Desk immediately.

Individuals sending information out of the Trust via an internet service (e.g. e-mail, web pages, social media etc.) have a personal responsibility to take into account how that information may be read. In particular, care must be taken to avoid any language that may be discriminatory, offensive or libelous (This includes comments or material based on gender, age, sexuality, race, disability or appearance)

Person-identifiable or sensitive information (including service user medical data and staff records) must not be stored, transported or transferred in any form (including removable media and portable devices) without the necessary permissions, audit records and security protection (including the use of NHS standard encryption tools).

Any attempt to circumvent or bypass restrictions, monitoring tools or software controls, whether locally on a PC or elsewhere, will be considered a deliberate and premeditated attempt to breach Trust security protocols. This could result in dismissal.

Individuals who do not use their network account for a 6 week period will have their accounts automatically disabled. To re-enable a de-activated account individuals must write to the Assistant Director of IT and Systems and request that the account is re-activated. IT staff may wish to discuss the request with the individual prior to reactivating access.

Line Managers must ensure any important records are preserved before the request to close is made or within the 60 day inactivity period in order to comply with the Data Protection Act.

Individuals are responsible for maintaining the security of their own login and password. Individuals must not share their user name or password with anyone. If a breach of security is recorded under an individual's login the burden of proof will be on the individual to prove he / she is not responsible for the breach. The Trust enforces a number of restrictions around passwords:

- Network passwords expire every 30 days, and must be changed accordingly
- The minimum acceptable password length is 8 characters
- Passwords must meet complexity requirements and must contain a mixture

of three from any four lowercase letters, uppercase letters, special characters or numbers e.g. Trust01 or Health.

- Individuals cannot re-use any previous 12 passwords when prompted to update a password
- The minimum password age is 1 day
- After 3 unsuccessful login attempts an individual will be automatically locked out of the system for 30 minutes

Individuals must logout of the system when completely finished with the internet

/ e-mail service e.g. at the end of the day. Whenever an individual takes a break away from the PC, 'Ctrl / Alt / Del' must be activated to lock the PC. In instances where a previous user has left access to the PC open, any individual requiring use of that PC must ask the previous user to log out prior to commencing the new session.

3.2 VIRUS CONTROL

The IT Department or its nominated agents will ensure virus-protection software covers every device capable of connection to the Internet. The IT Department in accordance with the supplier's recommendations will undertake the regular updating of such software.

3.3 NHS CODE OF CONNECTION

The IT Department or its nominated agents is responsible for maintaining a safe and secure computing environment in the Trust. It is responsible for ensuring the Trust conforms to the NHS Code of Connection and has fully implemented the NHS Security and Access Policy.

Any requests for connection require prior application for the NHS code of Connection. This includes changes to connections for any external agencies currently connected. Connection approval will be dependent on supplying the means of connection and the security processes intended to maintain a secure connection. The IT Department is responsible for arranging connection.

Other than that approved by the Department of IT and Systems no Trust PC or PC within the Trust managerial remit will be connected to external networking.

3.4 PROCEDURE FOR ACCESS TO INTERNET AND EMAIL SERVICES

Any individual requiring access to the Trust's network, email or internet services must apply to become an authorised user. This is activated via the online request and authorisation process for a new user account, accessed via the Intranet.

The Initial request can be completed on-line by any ELFT staff member using the above link. This will be followed by an automatic authorisation request email to the individual selected to authorise the account from the authorised list of signatories. The email includes a link to an on line template that allows the request to be accepted and authorised, or cancelled and rejected.

The authorisation will generate an automatic request to the IT Service Desk to set up the New User account. The above actions and authorisations will be recorded on a central server.

All users must read and agree to the Network, E-mail and Internet Use policy (this policy). By logging onto the network and clicking OK, users are confirming that they have read, understood and abide by the protocols contained within.

Individuals requiring access to national clinical systems are required to complete a similar declaration on an RA01 supporting form. Further guidance can be found in the "Registration Authority Policy and Procedure"

Access to the internet and e-mail is accessible only through the Trust firewall. If the PC is connected to the Trust network, access to the internet through a modem is not permitted.

3.5 USE OF THE INTERNET

Inappropriate content - Individuals are not permitted to access, display or download material from Internet sites that hold offensive or inappropriate content, or to send or knowingly receive such material by e-mail. This is a serious breach of Trust security and may result in dismissal. Offensive material is defined by the Trust's Equal Opportunity and Harassment Policy and includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The list is not exhaustive. Other than instances that demand criminal prosecution, the Trust is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet.

The Trust reserves the right to monitor staff use of the Network, Emails and the Internet and will take appropriate disciplinary action if activity is found to be non-compliant with this Policy.

Responsibility – Whilst access to the internet for Trust staff is not filtered or blocked, the availability of a site does not remove an individual's responsibilities for ensuring safe and appropriate use of information.

Downloading of Files from the Internet - Individuals who intentionally introduce files that cause computer problems could be prosecuted under the Computer Misuse Act:

- File downloads and transmissions via e-mail must be done in accordance with the laws which protect copyright, designs and patents.
- Download of Executable files is prohibited
- It is a breach of security to download, send or knowingly receive files which disable the network or which have the purpose of compromising the integrity and security of the Trust networks and file servers.
- The Trust IT network must not be used for the download, storage or transfer of personal music, video or photofiles.

Unintentional breaches of security

If an individual is unintentionally connected to a site containing sexually explicit or otherwise offensive material, the individual must disconnect from the site immediately and inform the Assistant Director of IT and their Line Manager. Where necessary an incident form must be submitted on Datix (as per the Trust's Incident Reporting Policy).

Information for service users - Individuals must seek appropriate advice from their Line Managers/clinical colleagues to confirm that any information obtained via the internet and intended for use by service users or the general public is accurate, timely and relevant to the intended need.

Use of the Trust's Name - Individuals participating in an online discussion are expected to conduct themselves in an honest and professional manner. Individuals are personally responsible for what is written. It is therefore important to be courteous and inoffensive, and to think twice before writing an angry e-mail or contribution to a discussion. Unless specifically authorised to do, individuals are not permitted to write or present views on behalf of the Trust. This means individuals cannot join a chat group in the name of the Trust, and cannot design a web site from a home PC and then publish it under the name of the Trust.

Use of social networking or blogging sites – Blogging and social networking sites present an easy means for information to leak from the Trust. Risks include unauthorized disclosure, identity theft, legal liability from defamatory postings, and reputational damage. Staff must be cautious in any postings, and if in doubt check with their line manager or the communications team before posting.

3.6 USE OF EMAIL

Electronic transfer of person identifiable information is only permitted on a person- to-person basis across secure networks or by encrypted disc addressed or delivered specifically to the intended recipient (Information Governance and IT Security Policy).

An NHS directive states that any information sent electronically must be encrypted. Sending important, sensitive or confidential information as an encrypted attachment by encrypted email is the safest way to send information electronically. Within the NHS there is a free-to-use encrypted email service called NHSMail which uses a NHS.net email address, available to all staff (for life). Generic email addresses are also available, as are secure addresses for associated companies (for example suppliers of prosthetics, pharmaceutical products etc.).

It must be stressed that sending information to another Trust by the usual firstname.lastname@trust.NHS.UK email address is NOT secure. Neither is it secure to send emails to local.government@gov.uk addresses.

The reason for this is that emails are only secure when they stay within the Trust (stay on the Trust's secure email server), or are transferred via the National Infrastructure N3 network. As soon as they leave the secure email server they travel via the internet and are susceptible to hacking

Other public services have similar secure email systems and those that are totally compatible with NHSMail can be used to communicate securely with other organisations such as Police, Courts, Local & Central Government. These secure emails use the N3 network, maintained as part of the National Infrastructure framework and used by the government and military services

It is possible that dozens of copies of the email and attachments are stored on internet servers all around the world, and those servers are

not well protected against hackers.

For sending/receiving secure emails, there is just one decision to be made, which depends on the recipient's email address:

3.7 TO SEND/RECEIVE BETWEEN SECURE EMAIL SERVICES (FROM NHS.NET TO NHS.NET OR ANOTHER SECURE GOVERNMENT APPROVED EMAIL ADDRESS)

Use NHS.net and securely communicate by email with any of the Government approved email domains. The full list of secure Government email systems as at September 2015 is shown below. They have email addresses ending:

- .cjsm.net (Criminal and Justice)
- .gcsx.gov.uk (Local Government/Social Services)
- .gse.gov.uk (Central Government)
- .gsi.gov.uk (Central Government including Department of Health)
- .gsx.gov.uk (Central Government)
- .hscic.gov.uk (The Health and Social Care Information Centre)
- .mod.uk (Military)
- .nhs.net (NHSmail)
- .pnn.police.uk (Police)
- .scn.gov.uk (Criminal and Justice)

3.8 TO SEND/RECEIVE BETWEEN NON-SECURE EMAIL SERVICES (FROM NHS.NET TO AN EMAIL ADDRESS THAT IS NOT A SECURE GOVERNMENT APPROVED EMAIL ADDRESS)

Use the [secure] feature of NHS.net to send emails to any email account (for example Hotmail, Gmail and Yahoo accounts even addresses in other countries, and those ending with nhs.uk that are not ELFT addresses) securely encrypted.

This is explained in the NHS.net Help, but in summary you simply use your nhs.net account and put the text [secure] including the square brackets as the first part of the email subject.

When you receive such an email you will have some instructions to follow (the first time only), and you'll be able to exchange such emails securely with the recipient.

If you are using your NHS.net account and communicating with any of the Government approved email domains in the above list, this [secure] feature does not work and in any case is not necessary.

3.9 TO GET AN NHS.NET ACCOUNT

All NHS staff should have an NHS.net secure email account. Get yours by logging a ticket with the ELFT Service Desk, then as soon as it is set up (usually by the next day) you will be able to use that nhs.net account wherever you are.

The account stays with you forever and can move with you as you go from Trust to Trust. Assistance with NHS.net accounts is handled by the Local Systems Administrator who can be contacted via the IT Service Desk

Please note that in some places it is referred to as NHSMail, in others it is NHS.net. They refer to the same system.

New NHSmail email encryption feature: secure email from NHSmail to non-accredited or non-secure email services

NHSmail already provides a secure method of exchanging sensitive information with other NHSmail users and public sector contacts that use one of the other secure Government email services (e.g.

.gcsx.gov.uk for Local Authorities).

Now, a new encryption feature means that NHSmail users can also securely exchange sensitive information with users of non-accredited or non-secure email services, for example those ending in nhs.uk, Hotmail, Gmail and Yahoo.

The new NHSmail encryption feature means that health and social care staff now benefit from a secure service which allows them to communicate across organisation boundaries and industry sectors. NHSmail can now be used securely across the entire health and social care community – in fact with anyone using any email account.

With the new NHSmail encryption feature:

- * NHSmail users can easily communicate securely with users of ANY email service including those ending .nhs.uk without having to manually encrypt sensitive information
- * Users can send attachments which will automatically be encrypted for you and remain secure
- * Organisations can save money by replacing existing post, fax and phone-based processes with secure email
- * Users of non-accredited or non-secure email services can communicate securely with NHSmail users saving time and money, speeding up communications and improving patient care
- * Communication is faster, easier and more reliable.

4.1 FURTHER GUIDELINES

Content must be appropriate – e-mail chains not relevant to the message must be deleted, and attachments must contain only the minimum information required. Large attachments must be avoided.

Consent of data subjects must be obtained – where required, consent must be obtained prior to the information being sent

Person identifiable emails must be classed as “Confidential”

Person identifiable information i.e. the name of a service user, member of staff, or other person must not be used in the title bar. Names may be used with caution in the body of the message where use of a pseudonym, numerical identifier or initials could cause confusion.

The Request Read Receipt option within the E-mail system can be used to confirm the recipient has received the mail

Storage and retention of the e-mail must be appropriate where it forms part of a primary record or decision trail (e.g. a print out in Service User case notes or Staffing files).

Circulation or forwarding of e-mails to large groups is carefully controlled. Individuals must **not** initiate large circulations unless they are authorised to do so for business purposes or without prior consultation and agreement with the Trust's Head of Communications who would normally deal with matters of public/general interest. Individuals must not 'reply all' to large groups where not necessary – misuse of this function has previously led to technical problems with large volumes of email in circulation.

Where it is essential to use e-mail to send personal information, individuals must ensure that: -

- The intended recipient has a legitimate need to know the identity of the person to whom the information refers
- The intended recipient has a legitimate need for the information
- The transmission route is secure i.e. through encryption
- The e-mail recipient can receive and store the e-mail securely – e.g. individuals must NOT send e-mails containing personal and sensitive information to their home e-mail accounts. Home PCs and personal e-mail service providers cannot guarantee security to NHS standards. This also contravenes the NHS Code of Confidentiality.
- Where necessary – the information sent is anonymised so that individuals referred to can only be identified or deduced by the intended recipient.

Managing email accounts - Individuals are personally responsible for managing their mailboxes effectively. Effective management of mailboxes is required to ensure the Trust meets its statutory obligations in respect of Data Protection, Freedom of Information and other legislation. The Trust's Records Management Policy also sets out specific requirements for storage and retention of records that require e-mails to be stored in an appropriately structured manner. Guidance on management is located on the Trust intranet. Additional guidance is available from the Head of Information Governance.

Non records emails must be proactively moved to storage folders or archived, and must additionally be reviewed on a regular basis.

IT Department responsibilities - The IT Department and its agents will ensure:

- The email system is reliable, up to date and resilient.
- Details held on the system are correct and complete.
- Only staff with a need to communicate externally will be given access to off-site communications.
- Other relevant organisations are informed of security incidents and issues.

4.2 ENCRYPTION

Attachments or bulk transfers of person identifiable or sensitive information sent over a non-secure network or by removable media, (including data memory sticks, CDs and DVDs) must be encrypted.

Laptops and removable hard drives must also be encrypted

4.3 ENCRYPTED USB MEMORYSTICKS

Individuals who can demonstrate a need for using information away from their substantive work location and where access to Trust network drives and systems may be difficult are permitted to transport information on a Trust encrypted

USB datastick. USB datasticks must not be used for transporting PID without the specific permission of the Information Governance Manager or Caldicott Guardian. Information stored on a Trust encrypted USB datastick must not be saved onto any computer that is not supplied by the Trust.

Disciplinary action may be taken against anyone failing to comply with this instruction.

Only encrypted USB datasticks provided by the Trust's IT Department may be used for Trust purposes. Disciplinary action will be taken against anyone using a personal, unencrypted USB datastick. Individuals are required to obtain authorisation from the Head of Information Governance by completing an on line application prior to issue and are required to sign to authorise receipt of. Encrypted USB datasticks can then be procured through the IT Department.

Individuals are required to set up an encryption code prior to use. The IT Department does not have access to this password. Individuals must not write this password down and must therefore commit the password to memory. If the password is forgotten, the IT Department can reformat the USB but this will wipe its contents.

Use and ownership of the encrypted USB datasticks is regularly monitored.

Other general principles and expected good practice applying to all services include the following:

Emails and other electronic forms of information may be used as evidence, made available to the general public under Freedom of Information legislation or to service users under the Data Protection Act's Access to Records requirements. Court Orders may also be obtained for access to information for legal purposes. The writing style must always be courteous, business like and brief.

Whilst individuals are allowed to use the e-mail system to send/receive the occasional private message, these messages and other information stored, sent or received on the Trust's IT services and resources could be accessed if:

- There is an investigation into an individual
- Access is needed to important messages whilst individuals are absent
- There is a routine audit of e-mail/internet/IT service usage

Emails that form part of a decision/audit trail or a patient/staff/personal record must be saved as above to a suitable electronic/physical place of storage and retained in line with the Trust's Records Management Policy and other supporting policies that cover electronic document creation, management and

storage.

All portable/mobile devices such as laptops, Smartphones and encrypted USB datasticks must be returned to the Trust when an individual leaves the Trust.

4.4 CONFIDENTIALITY AND SECURE STORAGE OF DATA

Individuals are bound by the Trust's Information Governance and IT Security Policy, and by the common law duty to maintain confidentiality concerning the data and information used during every day work within the Trust.

Under the Data Protection Act individuals may not disclose any information relating to a living identifiable individual. This includes both service users and staff. Additionally, individuals may not disclose confidential information relating to any aspect of the business of the Trust.

4.5 PERSON IDENTIFIABLE AND SENSITIVE DATA

Must not be stored on a PC's Local drive (C: drive)

Electronic copies requiring retention for legitimate business purposes must be kept in a secure network location agreed with the Line Manager – e.g. limited access Department I: Drive or K: Drive folder. They must not be stored on a personal H: Drive Must not be downloaded onto removable media or transferred to other locations, systems or organisations unless the individual is authorised to do so by the Caldicott Guardian or Head of Information Governance and is using approved encryption protection. Storage and retention of Emails that are records

To manage e-mails effectively, individuals must identify e-mails that are records and those that are not. It is important that e-mails that are records are transferred from personal mailboxes to the relevant clinical system or business records drive, and managed as part of those functions.

Emails that are records must be organised with similar types of information and retained according to the records retention schedule for records of that type.

If an e-mail has an attachment, the e-mail, the attachment or both could be a record. Usually the attachment must be captured as a record together with the e-mail itself as the e-mail will provide the context to the attachment.

A record is 'information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of businesses. To decide if an e-mail message constitutes a record, the context and content of the e-mail message must be considered.

Emails that are records are those that form part of a decision/audit trail or contribute to a service user/staff/personal record. They may include discussions regarding a business transaction or background information. They must be archived to a suitable electronic/physical place of storage and retained in line with the Trust's Records Retention and Disposal policy.

4.6 MANAGEMENT OF SECURITY

The Assistant Director of IT is responsible for physical security of IT assets. The Head of Information Governance is responsible for confidentiality and security of information.

IT System Owners have responsibility for:

- The protection of IT assets, information and systems within their department or for which they have responsibility.
- Ensuring the performance of specific security processes or activities, which relate to the system they are responsible for

4.7 GENERIC EMAIL ADDRESSES

There are occasions when it is appropriate for staff to share an email account so that, for example, it is not necessary to know the names of staff who work in Information Governance, but instead it is possible to contact the staff who work there by using the generic email address elft.information.governance@nhs.net.

This generic email address will be accessible to those staff granted access to it and who will receive the password allowing each of them to access the generic mailbox.

When the account is created, ownership must be established and it is imperative that the owner keeps a record of each staff member who has access to it. When a staff member must no longer have access to the mailbox the owner must ensure that access is removed otherwise the Trust is at risk of a former staff member having inappropriate access to the email system.

Examples of this include, but are not limited to, situations when they change their role or responsibilities within the same department, move to another department within the Trust, leave the Trust or leave the NHS. In cases such as these the generic mailbox owner must ensure that the access they previously granted is revoked.

All requests for generic email accounts must be made to the IT Service desk who will send a copy of the request to the generic Information Governance mailbox elft.information.governance@nhs.net seeking approval for the account to be created.

A generic account must only be used for the purpose intended and all staff having access to it must be trained by the email address owner and made aware of the reason for these accounts, and must agree to notify the email address owner when access is no longer required.

Authorised users of generic accounts must ensure that local policies and procedures are in place to protect privacy and confidentiality of all personal and sensitive

information. Such sensitive information includes all Person Identifiable Data.

A generic **NHSm**ail account can be set up and be used to send and receive sensitive emails on a regular basis. As NHSm

ail is used throughout the NHS there are naming conventions which must be followed, and there are specific procedures to be complied with, details of which are available from NHSmail Local Support.

4.8 INVESTIGATION OF NETWORK, EMAIL OR INTERNET USE

Monitoring - Use of all internet, e-mail and similar services is subject to an audit trail and will be investigated at the request of line managers

Audit - Audit tools will log by user name and password the time of day sites were accessed, for how long, and if a file transfer took place.

Excessive use - excessive use of the internet will be investigated at the request of a Line Manager.

Accessing offensive sites – If a request to investigate an individual's internet access is received from a line manager, and access to offensive sites is discovered, a full enquiry will be undertaken which may result in disciplinary action. When a breach is identified, the access of the person(s) involved will be suspended pending the enquiry conclusion at which point it may be terminated.

Breach of confidentiality/security – checks will be made on secure transit, storage and encryption of person identifiable and sensitive data

Availability - All individuals must make their system(s) available at any time for audit either by the IT Department, Internal Audit or representatives of the central NHS Information Authorities or any other body sanctioned by the Trust.

Purpose - All such audits will be for security purposes. If there is any doubt on validity of an auditor's actions or requests, individuals must contact the Assistant Director of IT and request confirmation of the impending audit.

Incident reporting - Breaches must be reported through the appropriate Line Manager and recorded via the Trust's Incident Reporting procedures.

Suspected breaches of security - Breaches or suspected breaches of security, abuse of service or non-compliance with the Trust's Network

Internet and E-mail Usage Policy or inappropriate use of Internet services, as judged by a Line Manager, will be investigated.

Applications for access require Service Director and Head of Information Governance approval and must be submitted using the on line intranet request form at http://elftintranet/it_support_and_services/ict_request_to_access_user_information.asp

The Information Governance Manager may carry out checks with the Human Resources Dept, Service Director, Caldicott Guardian or other appropriate individuals prior to releasing the information

- Access will be gained in the presence of a nominated IT staff member with a suitable witness where appropriate.
- A record will be made by the Information Directorate of the reasons for accessing the mailbox together with the names of the people who were present.
- The individual whose mailbox was accessed may be given a copy of the request form.

4.9 ACCESS TO E-MAIL ACCOUNTS

Individuals must ensure business continuity during planned absence. Line managers will advise individuals whether this must be by allowing trusted third party access to the account, or through an auto forward to a shared or colleague's email account.

It may be necessary occasionally to access an individual's mailbox. For example, if an individual is unexpectedly away from the office for an extended period and has not set up any alternative arrangements for access. Purposes for accessing an e-mail account could be to action:

- A Subject Access request under the Data Protection Act
- A Freedom of Information request
- Evidence in legal proceedings
- Evidence in a criminal investigation
- A Line of business enquiry
- Evidence in support of disciplinary action

Disciplinary procedures - Action from any investigation may result in the withdrawal of internet or e-mail services to an individual or a group of individuals, and could lead to further investigation and subsequent dismissal under the Trust's disciplinary procedure. Ultimately it may be necessary to proceed with criminal charges depending on the nature of the incident.