East London NHS
NHS Foundation Trust

NETWORK, INTERNET AND E-MAIL USAGE POLICY

Version 9

March 2015

DOCUMENT CONTROL SUMMARY

Title	Internet and E-mail usage policy
Purpose of document	To describe user rights and good practice to Internet, e-mail and mobile device users within the Trust
Reference (author)	N/A
Reference (network)	Intranet
Status	Draft
Version No.	9
Date	March 2015
Authors	Daniel Woodruffe – Associate Director ICT Tony Monachello – Head of Information Governance
Approved by (Name and title)	Information Governance Steering Group
Next Review Date	April 2016

VERSION CONTROL SUMMARY

Version	Date	Comment/Changes
1.0	2/10/2000	Draft reviewed by Executive Team on 9th November and for review by JSC on 15th November. This document was intentionally brief in order to set out and agree guiding principles
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 and to JSC for consultation and comment
3.0	13/11/2000	Working draft with minor changes – to be presented to JSC for approval in December 2000
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 access to services
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 page 9 – 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 updated
3.7	Jan 05	ANNEX 5 added – managing e-mail accounts in accordance with Freedom of Information Act & Data Protection Act - RK and additional comments from SP
3.8	May 05	Minor changes following discussion and approval at IG Steering group (e-mail security and user responsibilities) and to ensure consistency with other Policies
3.9	Aug 05	Include line manager authorisation which requires the line manager to advise the ICT Department when the user leaves the trust so that the users account may be disabled
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 ELCMHT. Alteration to formatting to streamline policy
4.1	Nov 05	General update and alterations to accommodate IG toolkit requirements. Main changes to Trust policy on e-mailing of person identifiable and sensitive information
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 users
5.1	Dec 2007	Expansion of expected practice covering confirmed national standards for encryption and limits to use of removable media
5.2	Jan 2008	Updated following comments and queries from

		users, additional info on NHSmail and confirmation of WinZip 11.1 and e-mail Companion order. Added reference to Connecting for Health document for third parties.
5.3	July 2008	Added information regarding Government domains that can receive encrypted e-mails from NHS.net e-mail accounts
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 Forms to end of document
7.0	February 2009	Streamlined to reflect short policy and fuller procedures format following comments and queries from users. Best practice guidelines removed to supporting guidance leaflet. Additional sections on return of equipment and use of USB devices added. Access and monitoring of accounts strengthened Third Party Access arrangements added Mandatory training requirements added Deactivation of accounts altered from 90 to 60 days Access to network accounts authorisation changed
7.1	March 2009	Deactivation of accounts altered to 6 weeks
7.2	February 2010	4.8 Additional section on blogging / social networking added 4.9 Clarification provided on using person identifiable information in emails 4.11 Instruction on obtaining a USB stick, transporting person identifiable information on USBs, and monitoring of use added 4.15 Clarification provided on Information Security responsibilities 4.17 Procedure for gaining access to users' accounts strengthened
7.3	May 2010	4.11 Instruction on USB use strengthened
7.4	March 2013	Updates to entire document: - Removal of references to legacy equipment (e.g. PDAs) - Improved formatting
9.0	March 2015	Reference to secure emailing options and general policy review.

CONTENTS

1. Purpose of this Policy

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 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 safe usage within the overall Information Governance framework which includes the Information Governance and IM&T Security Policy, Records Management and Freedom of Information Policies of the Trust. It should be used in conjunction with these and any other relevant policy documents and procedures. It should also be used in conjunction with Trust issued best practice guidance.

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

2. Key points of this Policy

- Person identifiable or sensitive information, where not anonymised, should only be sent via a secure email transmission method, as below, or encrypted (see appendix A).

    a. From one eastlondon.nhs.uk account to another eastlondon.nhs.uk account
    b. From one nhs.net account to another nhs.net account
    c. From an nhs.net account to a secure government domain (such as gsi.gov.uk, gsx.gov.uk, pnn.gov.uk, scn.gov.uk)
    d. Via Egress Switch to other parties who use this system
    e. To name.name@newham.gov.uk (a secure link is established between the Trust and Newham Council)

- All network services are primarily for work related activities. Limited personal use is permitted providing it does not interfere with work performance;
- Junk mail should 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 should be concise and business like;
- E-mail boxes should be regularly checked and cleared;
- Inactive accounts will be de-activated after 90 days;
- Passwords must not be shared under any circumstances;
- PCs should not be left unattended without being logged off or locked down (ctrl/alt/delete);
- E-mails that are records should 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;
- Information security or confidentiality breaches should be reported via the Trust's incident reporting system;
- Failure to comply with this policy may result in disciplinary action being taken, which may result in dismissal or criminal prosecution;
- 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 datasticks should be used. Individuals should not use any other datasticks whether or not these are encrypted;
- Current best practice guidance must be followed at all times

3. Definitions

3.1 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 should not attempt to gain access on unauthorised equipment, or without a username or password.

3.2 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.

3.3 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.

3.4 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, bleeps 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.

3.5 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.

4. Principles and Responsibilities

4.1 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.

4.2 Username and password management

The IM&T 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

4.3 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.

4.4 Personal responsibilities

Individuals have a responsibility to ensure copyright and licensing laws are not breached. Consequently, individuals should 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 should 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 IM&T 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 should 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 Associate Director of IT and Systems and request that the account is re-activated. ICT 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 7 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 H#ealth.
- Individuals cannot re-use any previous 12 passwords when prompted to update a password
- The minimum password age is 1 day
- After 5 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' should be activated to temporarily lock the PC. In instances where a previous user has left access to the PC open, any individual requiring use of that PC should ask the previous user to log out prior to commencing the new session.

4.5 Virus control

The IM&T Department or its nominated agents will ensure virus-protection software covers every device capable of connection to the Internet. The IM&T Department in accordance with the supplier's recommendations will undertake the regular updating of such software.

4.6 NHS Code of Connection

The IM&T 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 IM&T 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.

4.7 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.

4.8 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.

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 should not be used for the download, storage or transfer of personal music, video or photo files.

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 Associate Director of IT and their Line Manager. Where necessary an incident form should be submitted on Datix (as per the Trust's Incident Reporting Policy). .

Information for service users - Individuals should 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 should be cautious in any postings, and if in doubt check with their line manager or the communications team before posting.

4.9 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 IM&T Security Policy)

Internet / e-mail services provided over the public internet are not secure and therefore cannot guarantee safe transfer of confidential information.

E-mail users have a duty of care to preserve the confidentiality of personal information.

The use of e-mail to transmit personal/sensitive information should usually be avoided, and alternative methods used – e.g. shared network drives.

E-mails must be addressed ONLY to the intended recipient(s) – individuals should ensure the address is correct before pressing "send" and avoid using "Reply all" functions unless absolutely necessary

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

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

Person identifiable emails are marked "Confidential - addressee only" in the title bar

Person identifiable information i.e. the name of a service user, member of staff, or other person is not 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 should **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 should 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 should 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 should 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 should be proactively moved to storage folders or archived, and should additionally be reviewed on a regular basis.

IM&T Department responsibilities - The IM&T Department and its agents will ensure:

- The mail 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.

4.10 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 prior to sending.

Laptops and removable hard drives must also be encrypted

Encryption must be supported by use of a “strong” pass phrase or key containing:

- Minimum of 12 Characters
- Mixture of upper/lower case
- Mixture of alphanumeric and numeric characters

The pass phrase/key must not be sent by email. It must be relayed to the recipient of the data via a different route than the data file (usually telephone).

The minimum standard for encrypting person identifiable or sensitive data for bulk transfer, storage on removable media, transit or transmission by e-mail is using 256-bit AES encryption. This standard will be updated from time to time and notified to staff.

The list below defines the **only** acceptable options for sending personal / sensitive information. No other methods should therefore be used:

- From one *eastlondon.nhs.uk* to another *eastlondon.nhs.uk* e-mail account. e.g. name.name@eastlondon.nhs.uk to name.name@eastlondon.nhs.uk . This should only be used for the transfer of personal information within the Trust. It should not be used to transfer personal information outside the Trust
- From one NHS.net e-mail account to another NHS.net e-mail account e.g. name.name@nhs.net to name.name@nhs.net The nhs.net mail system is specifically designed for the transfer of personal or confidential information and should be used when sending such information to a member of another NHS organisation. Some local authority staff also have access to nhs.net e-mail accounts. However, individuals should ensure that the recipient has an nhs.net account prior to sending the information. Individuals should not send personal information from an nhs.net account to a non-nhs.net account. Please note – e-mails between eastlondon.nhs.uk and any external e-mail address including other nhs.uk and nhs.net accounts, *are not encrypted,* therefore not considered secure and should therefore NOT be used. Details on how to obtain an NHS.net e-mail address can be found at https://www.nhs.net/ using the “Register here” function.
- From an NHS.net e-mail address to the following secure Government domains - *.gsi.gov.uk e.g. name.name@nhs.net to name.name@gsi.gov.uk *.gsx.gov.uk, *.gse.gov.uk, *.pnn.gov.uk, *.scn.gov.uk, *.pnn.police.uk, *.eu-admin.net, *.gsisup.co.uk, *.cjsm.net, psops.net.
- Via Egress Switch to other parties who use this system (contact IM&T for further information)
- To name.name@newham.gov.uk (a secure link is established between the Trust and Newham Council)
- Encrypted using 7zip software – See appendix A

Individuals needing to encrypt sensitive files prior to dispatch or storage should seek advice from the Head of Information Governance

Please note that whilst passwords on Word/Excel files add some protection, they can easily be bypassed. Anonymisation of information should therefore be used where security of the transmission route is uncertain. Social Services and other agencies may have protected internal networks but e-mail messages sent from an eastlondon.nhs.uk e-mail account directly to Social Services will NOT be secure and should therefore be anonymised. Social Services staff may have access to NHSmail (nhs.net) e-mail accounts. This is the preferred method of e-mailing personal or confidential information.

4.11 Encrypted USB datasticks

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 should not be used for transporting person identifiable information 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 IM&T Department should 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 than be procured through the IM&T Department.

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

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

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

E-mails and other electronic forms of information could 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 should 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 IM&T 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/IM&T service usage

E-mails that form part of a decision/audit trail or a patient/staff/personal record should 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.

4.13 Confidentiality and Secure Storage of Data

Individuals are bound by the Trust's Information Governance and IM&T Security Policy, and by the common law duty to maintain confidentiality concerning the data and information used during everyday 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.

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 should be kept in a secure network location agreed with the Line Manager – e.g. limited access Department I: Drive or K: Drive folder. They should 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 should 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 should 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 should 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 business'. To decide if an e-mail message constitutes a record, the context and content of the e-mail message should 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 should be archived to a suitable electronic/physical place of storage and retained in line with the Trust's Records Retention and Disposal policy.

4.14 Management of security

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

IM&T System Owners have responsibility for:

- The protection of IM&T 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

4.15 Access to e-mail accounts

Individuals should ensure business continuity during planned absence. Line managers will advise individuals whether this should 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

4.16 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 p e r s o n identifiable and sensitive data

Availability - All individuals must make their system(s) available at any time for audit either by the IM&T 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 Associate Director of IT and request confirmation of the impending audit.

Incident reporting - Breaches should 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 should be submitted using the on line intranet request form at http://elftintranet/it_support_and_services/ict_request_to_access_user_information.asp

The Head of Information Governance may make 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 IM&T 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.

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.

East London NHS
NHS Foundation Trust

APPENDIX A

Encrypting your files using 7-Zip Software

To increase the level of security, you can encrypt a file before sending it via email. Encryption is a software tool that uses "scrambling" to make data unreadable. Once a message is encrypted, it will appear as a meaningless garble of characters to anyone except the person who has the password to unscramble it.

- Launch 7-zip using the Start menu (Start - All Programs - 7-zip - 7-zip file manager).
- In the 7-zip file manager locate the file that you want to encrypt (the file manager will list all storage drives).
- Once you have located the file you want to encrypt, select it by clicking it once.
- With the file highlighted, click 'Add.'
- This will open a new window called 'Add to Archive.'
- At the top of the left column change the 'Archive Format' to 'Zip' using the drop-down menu.
- At the bottom of the right column check that the 'Encryption method' says 'AES-256.'
- Above it, type your chosen password into the 'Enter password' text box.
- Directly beneath it, re-enter your password into to the 'Re-enter password text box.
- Click 'OK' to close the 'Add to Archive' window.'
- Back in the file manager you can now see the encrypted and zipped file. You can identify it by its icon which is of a folder with a zip through it.
- You can now send the file as an email attachment but remember **not to include the password** in the same email.

Opening an encrypted file

To open an encrypted file via email attachment you will need to use 7-zip or WinZip.

- In the email message window double click the zipped attachment.
- You will then be asked if you want to open the attachment from its current location or save it to your computer. Click 'Save.'
- Save the file to your desired location.
- Close the email message window.
- Open 7-zip using the Start menu. This will open the 7-zip file manager.
- Browse for your encrypted file using the drop down list of file locations.
- Once you have located your file, double click it to open the folder.
- In the folder, double click the document to open it.
- At this point you will be asked to enter the password assigned to the encryption process. Enter the password and click 'OK.'
- You will then be asked to enter a password and click 'OK.'
- The Word document should now be open.