Lincolnshire Partnership
NHS Foundation Trust

Lincolnshire Partnership NHS Foundation Trust (LPFT)

ICT Systems Use Policy

DOCUMENT VERSION CONTROL	
Document Type and Title:	**ICT Systems Use Policy**
Authorised Document Folder:	**Corporate**
New or Replacing:	**ICT Systems Use Policy v3.2**
Document Reference:	**8c**
Version No:	**4.0**
Date Policy First Written:	**March 2013**
Date Policy First Implemented:	**March 2013**
Date Policy Last Reviewed and Updated:	**June 2018**
Implementation Date:	**August 2018**
Author:	**Head of Informatics**
Approving Body:	**Information Management and Technology Committee (IM&T Committee)**
Approval Date:	**13 August 2018 (proposed)**
Committee, Group or Individual Monitoring the Document	**IM&T Committee**
Review Date:	**August 2020**

ICT Systems Use Policy Executive Summary

This Policy provides direction on the use of ICT equipment for the processing, storing and retrieval of data throughout Lincolnshire Partnership NHS Foundation Trust (referred to hereafter as 'the Trust'); to ensure that all ICT use within the Trust supports the provision of high-quality service user care and business delivery, promotes the safe and effective use of resources, and protects the Trust's data and assets by achieving compliance with agreed local and national standards.

This policy sets down the basic standards for the use of ICT equipment that will be applied across the Trust, and outlines the responsibilities of the Trust, managers and each member of staff (staff members include paid employees, workers on honorary contracts, contractors, apprentices, volunteers, individuals on secondment and trainees).

Contents **Page**

Executive Summary 2

1. Introduction 4

2. Legislation, Guidance and Policy Documents Considered 5

3. Definitions and Abbreviations 5

4. Duties 7

5. Policy arrangements and Procedures 8

5.1 Rationale 8

5.2 Standards 9

5.3 Procedures 9

5.3.1 Access Control 10
5.3.2 Password Composition 11
5.3.3 Data Security and Cyber Protection 12
5.3.4 Equipment Security 14
5.3.5 General Computer Use 15
5.3.6 Personal Use and Privacy 16
5.3.7 Service User and Guest Access 17
5.3.8 Access to CED 18
5.3.9 Asset Control 19
5.3.10 Email 21
5.3.11 EIS Access Control 26
5.3.12 Mobile Phone 30
5.3.13 Staff Audit and Activity Investigations 34

6. Implementation 35

7. Monitoring 35

8. Associated Documentation 36

Appendix A: Guidance for Agreeing an E-mail Exchange with a Service User
Appendix B: Lincolnshire Partnership NHS Foundation Trust Managed EIS
Appendix C: e-Rostering Procedure

1. Introduction

1.1 Information, Communication and Technology computerised information systems are important Trust assets holding business sensitive and personal confidential information and as such it is essential to take all necessary precautions to ensure that they are at all times protected.

1.2 The Trust acknowledges that it must demonstrate to its stakeholders, its patients and the public its commitment to provide effective and secure computer systems throughout the organisation, for the delivery of care and services, to protect and where appropriate share information and knowledge in support of the Trust's mission and in order to conduct the Trust's business.

1.3 To facilitate safe, effective working the Trust allows all staff appropriate authorised access to its information systems and technology, including the Trust network, email and mobile technology. However, to mitigate any risks to the Trust, this policy sets out the standards applicable for the use of the Trust's ICT Systems, hardware and networks.

1.4 This policy and its procedures replaces all previous Lincolnshire Partnership NHS Foundation Trust (LPFT) Computer Use and related technology policies and should be read in conjunction with all relevant and referenced policies. It should be noted that this Policy does not cover Information Management and Security, and that this Policy can be accessed via the Trust's Intranet system, http://www.lpft.nhs.uk/assets/files/Accessing%20our%20information/Policies%20and%20Procedures/policy-8b-information-management-and-security-policy-final-uploaded-311017.pdf

1.5 All of the documents highlighted within this policy which are standard templates or forms which staff are expected to utilise will be hyperlinked to the Trust's SHARON site; Amendments may be made to all forms so stockpiles should not be created and the forms should be regularly re-accessed.

1.6 If you wish to make a suggestion regarding amendment to this policy please contact the author; details can be found on the front cover.

1.7 This policy, the procedures and the associated documentation have been approved by the IM&T Committee. They will be reviewed by this Committee every two years or sooner if required by changes to legislation or guidance. Trust Legal Services will maintain a version of old policies for the lifetime of the organisation + 6 years (they will then be moved to a place of deposit) in line with the recommendations contained within 'Records Management Code of Practice for Health and Social Care 2016'.

1.8 If staff are unsure of their responsibilities at any time they should discuss this with their line manager in the first instance. Further guidance and support can also be obtained from:

ICT Services: 0300 1231020
http://icthelp.lincolnshire.nhs.uk/
Email: it.supportdesk@gemcsu.nhs.uk

Informatics Service: 01529 222328
http://sharon/lpft/PI/default.aspx
Email: informatics@lpft.nhs.uk

2. Legislation, Guidance and Policy Documents Considered

2.1 This policy is not a substitute for the legislation, regulations and Codes of Practice to which all staff must adhere. The list below is not intended to provide a complete list of the legislation governing the practice of NHS employees but is guidance provided as a minimum.

Data Protection Act 2018
Data Security and Protection Toolkit standards
2017/18 Data Security Protection Requirements
Cyber Essentials – 10 steps to cyber security
Telecommunications Code 2017
National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs
Records Management Code of Practice 2016
Safe Data, Safe Care
Regulation of Investigatory Powers Act 2016
The NHS Confidentiality Code of Practice 2003
Department of Health Copying Letters to Patients Guidance 2003
Freedom of Information Act 2000
Electronic Communications Act 2000
Human Rights Act 1998
Computer Misuse Act 1998
Access to Health Records Act 1990
Copyright, Designs and Patents Act 1988
Health and Safety at Work Act 1974
The Public Records Act 1958
The Common Law Duty of Confidentiality
NHSLA Standards
British Standard for Legal Admissibility and Evidential Weight of Information Stored Electronically (BSI BIP0008)

2.2 This policy has been written in consideration of the Care Quality Commission Essential Standards of Quality and Safety.

3. Definitions and Abbreviations

3.1 Definitions

The Trust's ICT System comprises:

- All network infrastructure including cables, wired and wireless access points
- Network hardware including servers, storage and communications equipment
- Personal hardware, i.e. desktop PCs, laptops and tablet devices
- Printers including multi-functional devices
- Peripheral equipment such as keyboards, mice, digital pens and digital dictation machines
- All major software applications including all clinical systems, such as the eReferrals system, , Silverlink, RiO, IAPTus, and SystmOne
- All generally installed software, such as Microsoft Office applications, plus any additional software installed on Trust computers or servers
- Portable devices such as Smartphones, mobile phones, cameras and any other external device that can be connected either directly or wirelessly to the Trust's ICT infrastructure

- All removable media i.e. CDs/DVDs, memory sticks/flash drives, external hard drives and any other data storage device

Confidential Information comprises:

- **Person Identifiable Data (PID)** is any information that can identify a person. This includes our patients or service users, carers and our staff
- **Personal Confidential Data (PCD)** is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people
- **Sensitive Personal Data** means personal data consisting of information as to:

  (a) the racial or ethnic origin of the data subject,

  (b) their political opinions,

  (c) their religious beliefs or other beliefs of a similar nature,

  (d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

  (e) their physical or mental health or condition,

  (f) their sexual life,

  (g) the commission or alleged commission of any offence, or

  (h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

- **Corporate Sensitive data** is information about the business function of the Trust, which could be commercially valuable, such as financial or contracting information.

Removable Media: any portable device capable of storing data. This includes;

- Data storage devices such as:
  - CDs and DVDs
  - Audio and video tapes
  - USB Flash drives/memory sticks
  - External hard drives
  - SD memory cards or

- Any item of equipment containing one of the above storage devices as an integral component, such as:
  - Laptop/notebook/tablet computers
  - Cameras, both photographic and video
  - Dictation machines and audio tape recorders
  - Mobile phones and Smartphones
  - Telephone answering machines
  - Fax machines
  - Printers
  - MFDs

Cyber Security: Cyber security comprises of technologies, processes and controls that are designed to protect systems, networks and data from Cyber Attacks.

3.2 Abbreviations

CD – Compact Disc
DVD – Digital Versatile Disc
IAA - Information Asset Administrators
IAO - Information Asset Owners
IMT – Information Management and Technology
IT – Information Technology
ICT – Information Communications and Technology
MFD – Multi Functional Device
PC – Personal Computer
SD – Secure Digital
SHARON – Staff Hub and Resource Online Network http://sharon/Pages/default.aspx
SIRO - Senior Information Risk Officer
USB – Universal Serial Bus

4. Duties

Individual/ Group	Responsible For:
Chief Executive	As Accounting Officer of the Trust the Chief Executive has ultimate responsibility for staff and organisational adherence to legislation, guidance and policy and for ensuring appropriate mechanisms are in place to support service delivery and continuity.
Senior Information Risk Officer (SIRO)	The SIRO has to ensure that the Trust has robust policies and procedures in place to ensure security of information held and communicated at all times.
Information Governance Lead	Contributes to the formulation and implementation of this policy and advises on information issues which may arise from the monitoring of the policy.
Head of Informatics	The Head of Informatics is the owner of this Policy and will ensure the provision, maintenance and authorised access control of the Trust's computer systems.
Deputy Director of Informatics with the lead for IT Security	Ensures the security and integrity of systems owned and operated by the Trust.
Directors/Managers	Have responsibility for ensuring all staff have access to this policy.
Information Asset Owner	The IAO is a mandated role; the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately, making sure that information assets are properly protected.
Information Asset Administrator	The IAA supports the IAO to action authorised Access Request Forms, granting and revoking access to controlled systems in accordance with the guidelines for each system.
Human Resources	The Human Resources Department will provide a monthly leavers list to the IT Department.
Divisional Managers/Business Managers/	Are responsible for ensuring that;

Service Leads	• Their staff are made aware of this Policy and their individual responsibilities. • Staff are made aware of any local management requirements or restrictions. • They and their staff comply with requirements of this Policy and associated Procedures and Guidance.
All Staff	This policy applies to all full-time and part-time staff of the Trust, non-executive directors, governors, contracted third parties (including agency staff), students/trainees, volunteers, apprentices, and staff on secondment, staff on placement with the Trust, and staff of partner organisations with approved access. It applies to all areas in support of the Trust's business objectives both clinical and corporate. All staff have an individual responsibility to ensure they; • Are aware of and comply with this Policy and any local management requirements guidelines or procedures. • Know where to locate a copy of this policy when necessary i.e. policy manuals or on the Intranet/SHARON. • Are aware how this policy and procedures impact on their practice and be able to follow the specified requirements set out.
Information Management and Technology Committee	Approves and monitors all aspects of the policy. Receives reports and monitors standards as detailed in Section 7.
Information Governance and Records Management Group	Monitors relevant Information Governance aspects of the policy and elevate areas of concern and action plans to the IMT Committee

5. Policy arrangements and Procedures

5.1 Rationale

ICT Systems Use has the following fundamental aims:

- To maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within the Trust
- To promote the correct use of ICT to support the clinical, operational and administrative work of the Trust
- To identify and mitigate potential risks by providing guidance on acceptable use and best practice
- To highlight cyber risk and reinforce effective cyber security
- To ensure that the Trust complies with its legal obligations

- To ensure the security of Trust ICT systems and the confidentiality of the information they contain

- To safeguard the Trust against the risk of inappropriate or improper use of its resources

- Where standards or policy have been breached, to provide a process for action to minimise further risk to the Trust and individuals

- A breach of this policy may have serious consequences for the Trust, which may include loss of public confidence and legal or financial penalties. To counter policy breaches the Trust may invoke its disciplinary procedure, which may include civil or criminal proceedings and/or the reporting of incidents to external agency for review and potential action

5.2 Standards

- The provision of the Trust's ICT infrastructure including servers and identified systems is managed and maintained under SLA by Information Communications & Technology Services (ICT) provided by Arden and Greater East Midlands Commissioning Support Unit (AAGEM CSU). This includes the Local Area Network (the LAN).

- The Wider Area Network (the WAN) across Lincolnshire is delivered via a Community of Interest Network (COIN). The COIN is managed through a Lincolnshire Consortium of which the Trust is a member. United Lincolnshire Hospitals Trust manage the COIN on behalf of the Consortium.

- All access to the Internet from within the network is via the NHS wide National Network and must be operated in such a way as to protect the Trust's internal network and systems. The NHS wide National Network is currently N3 and is moving to HSCN (the Health and Social Care Network) during 2018.

- Access to the N3/HSCN network is provided through secure gateways, and the Trust's Wide Area Network management is in accordance with the NHS Statement of Compliance. The Trust operates a secure Firewall between the Trust's Local Area Network and N3/HSCN.

- Access to the Internet, external to the LAN, using Trust mobile devices, is only permitted on the proviso that no confidential information is accessed, shared or utilised with no downloads onto any Trust ICT equipment permitted. This access supports the corporately owned and personally enabled agenda but must be operated in such a way as to protect the Trust's internal network, systems and equipment.

- Virus protection: ICT will ensure that appropriate technical steps are taken to reduce the vulnerability of the LPFT network to attack from cyber-attack. Users have a vital role to play in recognising the cyber agenda and taking precautions whenever they are online to reduce the potential of them opening up the network to attack. Users should note in particular to be very wary of e-mails from addresses that they do not recognise and are not expecting; these emails may purport to have instructions to download an attachment or access a hyperlink. Unsolicited emails should be treated with suspicion and not be opened. Users are requested to report anything they deem to be suspicious to the IT Helpdesk.

- Access to the Trust's network is only permitted to authorised staff that have completed the registration process, obtained their own unique personal username and password, and if appropriate received training. Only the user's personal access credentials may be used to gain access to the Trust's network and computer system. Sharing of access credentials is **not permitted** under any circumstances and will lead to disciplinary proceedings.

5.3 Procedure

5.3.1 Access Control

Access to the Trust's network and computer systems is only permitted to authorised staff that have completed the registration process, obtained their own unique personal username and password, and if appropriate received training. Only the user's personal access credentials may be used to gain access to the Trust's systems.

Once a staff member has gained authorised access to a system their role may require them to access national and/or local applications, such as the eReferrals system, the Patient Demographic Service, the Lincolnshire Clinical Care Portal, ESR, Silverlink/RiO, IAPTus, SystmOne etc., or smaller local databases and spreadsheets. Request for access to these applications should be made to the appropriate system administrator and may require a separate username & password, or a Smartcard and PIN

Accessing or attempting to access any part of the Trust's Network, including national and local applications, using any method other than your own authorised personal user identifier and password, or Smartcard & PIN, will breach this policy

It is **not** permitted at any time to use another person's personal username and password or Smartcard & PIN to gain access to any part of the Trust's network or associated systems. The person whose log-on credentials are used will be held accountable for all actions during that login period to any Trust computer, system or application. Breaching this policy will result in disciplinary action for both parties

Personal passwords

Everyone granted authorised access to the Trust's network and its clinical and corporate systems is issued with a personal password, which forms part of his or her personal access credentials. Additional personal access credentials may be issued for access to corporate or clinical systems such as ESR or Silverlink etc.

All personal password holders are responsible for:

- Changing their supplied password on first log on to a unique personal password to make it secure
- Always keeping their password private and confidential
- Never sharing their password with anyone, this includes Trust senior officials, ICT staff, personal secretaries and locum staff
- Never writing down or recording their password where it can be accessed by anyone other than themselves. Recording passwords is not recommended; therefore passwords should only be recorded when absolutely necessary; the password holder is responsible for the security of this information
- Changing their passwords on a regular basis; a minimum of three monthly

Group or Shared passwords

are only to be used by exception.

It is accepted that sharing passwords may be required in certain circumstances to facilitate team working, for example, sharing departmental office applications and equipment, such as:

- Access databases
- Excel spreadsheets
- Word documents
- Department or Team external encrypted back up devices
- Training Room PC's & laptops

Group passwords must be managed by appropriate department/team managers and trainers with the consent of their Head of Department and only where:

- Access to a shared resource cannot be safely and effectively achieved in any other way
- All participants have physical access to the encrypted backup device, equipment or direct access to the folder containing the controlled shared document. All participants must first log on to the network/PC/laptop using their own personal access credentials before using a group password

In the case of training participants use of a shared login and password to access a training PC is permitted but only under constant supervision by a trainer and where there is no access available to confidential data without the further submission of a personal password.

Department or team managers of group passwords are responsible for:

- Formally documenting the requirement for a shared password
- Maintaining an up to date list of all staff issued with the password
- Advising each participant of the other password holders
- Changing the password on a regular basis; a minimum of 3 monthly.

Everyone using a group password is responsible for ensuring it is kept confidential and solely within the members of the group

Group passwords must NOT be used to grant access to any corporate or clinical LIVE system and, with the exception of training, any Office application, created in Access, Excel, Outlook, Word etc., or any other folders or files - unless they are part of a formal documented process as outlined above

5.3.2 Password Composition

Corporate and Clinical Electronic Patient Records (EPR) passwords
(ESR, RiO, IAPTus etc.)

- The appropriate System Administrator will supply passwords or update Smartcard roles for applications or systems with additional access control. They will advise you of any variation of format and composition for the password their system uses
- Issued passwords must be changed on first use to make the password unique and secure

Minimum requirement (simple password)

All passwords:

- Should be easy to remember and difficult to guess
- Must be a minimum of six characters long, which should be a combination of both letters and numbers, e.g.: A4Y8G3
- Must not be the same as your user ID
- Must not contain sequential characters, e.g.: ABC123
- Must not contain duplicated characters e.g.: AAA111
- Must not be similar to your surname or forename

NB: Use different passwords for different systems (including systems and applications outside of the work place); if your password is hacked this will limit the damage and impact to you and the organisation

Preferred password composition (complex password)

When complying with the minimum requirements a complex password becomes much stronger and more effective when:

- Between 9 – 6 characters long
- Contains three different types of character from these four categories:
  - Uppercase letters
  - Lower case letters
  - Numeric digits
  - Special characters.

Examples: FzC$18j3 or TiG149eR

It can also help to consider a phrase that is personal to you and easy to remember i.e. Iha103@tC (I have a 103 at the Chinese)

Changing Passwords

Everyone is responsible for changing **each** of their personal passwords

- **Immediately**, whenever there is suspicion a password may have been compromised
- When prompted to do so by the system they are using
- On a regular basis; at least every 90 days if not prompted otherwise

5.3.3 Data Security and Cyber Protection

Data created and stored within Trust Systems is one of the Trust's most important and valuable assets. Much of this data is very personal and the Trust has a legal obligation to maintain its confidentiality and security

There is much investment in maintaining the security of the Trust's network and data stores but there are regular targeted and random attacks on the NHS. All staff must be aware and vigilant in this respect and take personal responsibility for the protection of data.

All staff with regular network access should routinely store all their data within personal or team/departmental network folders
Staff must not store confidential data on the hard disk or C:\ drive of any computer unless:

- The computer has been encrypted, AND
- All data has been backed up appropriately to a secure Trust owned location beforehand (Suitable back-ups can include the server, encrypted data sticks and encrypted external drives)

To avoid any possibility of confidential data being saved to an unencrypted computer's hard drive by mistake, usually to "My Documents", it is strongly recommended that no information, whatsoever, of any type, is stored on an unencrypted drive

Where staff do not have immediate access to a network drive, they should store their data on encrypted external memory devices, such as encrypted USB memory sticks, which they are responsible for keeping securely. All staff have access to an home drive for work related personal storage; where staff need advice on how to access this they should contact the ICT service desk.

PID in Databases, Spreadsheets etc.:

To locate easily and avoid duplication in compliance with the Data Protection Act 1998, the Trust maintains an accurate and up to date register of all data stores containing PID. Therefore:

- DO NOT create Access databases, Excel spreadsheets or Word documents, to store or process PID without first seeking approval to do so from the Information Governance Lead within the Informatics Service on 01529 222322

Data Back up

To provide continuity of care and service, it is essential that all data is backed up on a regular basis to a separate device

- **Network storage:** The ICT department will undertake and manage the backing up of all network drives on a regular basis
- **Non-Network storage:** Staff who require additional data storage in addition to their home (H:\) drive are responsible for managing their own regular data back-ups e.g. with use of an encrypted external hard drive
- **Small storage requirement:** Staff who normally store their data on an encrypted USB memory stick, should consider backing up their data on an additional encrypted USB memory stick or encrypted external hard drive. Both USB devices should be appropriately labelled and secured separately on site

Requests for encrypted data storage devices should be made via the ICT equipment ordering services at http://sharon/lpft/PI/Pages/ICT-Equipment-Request.aspx

Data Back up

Larger or Team storage requirements: The first choice for a team should be the use of either a secure area on the server (Z:\\ drive) or an internal area on SharePoint (SHARON).

However where these options are not feasible, managers can consider a larger capacity encrypted external hard disk drive. Through a formal documented process these devices should be appropriately managed and used following the guidance for group or shared passwords in paragraph 5.3.1 above. Requests for encrypted external hard drives should be made via the ICT equipment ordering process at http://sharon/lpft/PI/Pages/ICT-Equipment-Request.aspx

Advice about the options for Larger or Team storage requirements may be obtained from the Informatics Service.

Confidential Electronic Data in Transit:

- All confidential data held in electronic format MUST be encrypted in transit; failure to do so is a breach of this Policy
- To enable continuation of care and service in the event of data loss in transit all confidential data must be backed up to a network folder or another external secure device BEFORE it is removed from the security of an NHS site.
- Confidential data should only be transported using one of the Trust's recognised encryption standards
- Users must also be aware that they have a legal duty to maintain the confidentiality of data/information taken out of the Trust for working offsite or at home, whether it is paper based or as computer files.
- When confidential data has been authorised, by your line manager, to be processed offsite, users are subject to the Trust confidentiality agreements and must ensure they meet the requirements of this policy, the Data Protection Act, the Trust Information Security Policy and the Confidentiality and Data Protection Policy.
- All Laptop/tablet computers that are used to process Confidential information **must** be Trust owned or managed.
- All mobile computer devices should be encrypted and asset tagged by ICT Services before use.
- All mobile computer equipment must be purchased through the ICT Department who will then configure the equipment in accordance with Trust baseline security measures before being used.
- No one other than an authorised user is to operate the system.

For physical transportation:

- ICT approved and installed encryption for PC
- Full-Disk Encryption for desktops and laptops ICT approved and installed encryption for File/Folder
- ICT approved and installed encryption for Mobile Devices
- ICT approved and installed encryption for Removable Media i.e. ICT supplied encrypted USB memory sticks and encrypted external hard drives

For email transportation:

- NHSmail email
- NHSmail Secure File Transfer (SFT) – (requires NHSmail account)
- 256 bit AES encryption of files attached to the Trust's email system using WinZip version 9 or above

Encrypted external USB devices used for data storage or backing up should not be routinely used to transfer data between sites unless the process has been agreed and documented with the Information Governance Lead within the Informatics Service on 01529 222322.

5.3.4 Equipment Security

To preserve the security of Trust's information asset ONLY Trust owned or formally contracted/leased hardware, software, media and related equipment may be used within any part of the Trust's Network including all fixed and mobile devices

Hardware, software or media NOT owned/contracted/leased by the Trust, MUST NEVER be installed or connected to any part of the Trust's Network including fixed and mobile devices

The above policy statement specifically prohibits:

- The installation or connection of any personally owned software, hardware or media by staff to the Trust's Network and IT equipment

Non-compliance may create an immediate major security breach, jeopardise the Trust's NHS network (N3/HSCN) connection with NHS England and may result in disciplinary action for the user

Media Security: Removable media should be stored securely at all times. Media containing data must be stored appropriately in accordance with the sensitivity of its content and in an equivalent manner that would apply to paper based documents; see paragraph 5.3.3 on data security

5.3.5 General ICT Use

Physical Security: All Trust staff will ensure that every reasonable precaution is taken to house and store all computer equipment, accessories and media securely both when in use, and in and outside of working hours. Before vacating work areas containing ICT equipment, this should be secured and external views of the equipment obscured with blinds or curtains. Staffs are urged to visually check their computer equipment daily and report any obvious tampering or discrepancies to the ICT service desk

Portable Equipment should always be locked away in cabinets or cupboards when not in use or outside working hours. Mobile staff must transport portable equipment in car boots out of view, where possible removing them from the car immediately on arrival for use or secure storage in a building. Where not possible the car boot should not be opened to display the contents and must be locked at all times. ICT equipment must be removed as soon as possible for use/secure storage (i.e. in a locked house out of sight when not in use) and never left in a car overnight.

General Protection: Never leave your ICT equipment unattended without locking it or protecting it against intrusion or casual observation

- All activity undertaken during a log in period will be attributed to the person who logged onto the network/equipment, regardless of who actually used the machine
- Where using a desktop/laptop device staff are strongly encouraged to log off and shutdown their equipment if they intend being away from their PC for a long period

Change Control: Refer all install requests to the ICT Service desk as only their technicians are authorised to add, remove or modify any part of the Trust's ICT equipment; infrastructure, hardware, or software.

- **Free/Demo/Trial Software:** may only be installed as part of a change control process or with the documented approval of a senior member of the Informatics Service.

Housekeeping: Everyone is responsible for regularly reviewing their own data storage areas removing unwanted files and freeing up storage space in conjunction with the Trust's document retention and disposal scheme (see the Records Lifecycle Management and Information Governance Policy). This applies equally to staff storing data on networks, local hard drive or removable media

Relocation & Asset Management:

- A Trust Asset Register is held of the ownership and location of every piece of ICT equipment. Any change in ownership or location must be reported to ICT services and a receipt obtained and retained by the previous registered owner in case of query.
- The owner listed on the ICT asset register is responsible for the update of the asset register and will be held responsible if any piece of ICT equipment, for which they are recorded as the owner, is missing and cannot be recovered.
- Upon leaving the organisation the manager of the member of staff leaving is jointly responsible for the recovery of all ICT equipment and the return of this to ICT services (receipted) or the redeployment of kit, which must also be reported to ICT services for the ICT asset register maintenance.

Specific Exclusions:

The Trust Network and ICT equipment is NOT to be used:

- For any purpose which conflicts with any Trust Policy, Professional Code of Conduct or your contract of employment
- For any potentially illegal, improper or unacceptable use, such as creating, receiving, viewing, copying, transmitting or holding any obscene or offensive material or material calculated to incite racial or religious hatred, etc.
- To introduce malicious software, such as viruses, into the Trust Network
- For knowingly making untrue, inaccurate, misleading, offensive or potentially defamatory statements about any person or organisation

Knowingly using the Trust ICT system in this way will lead to disciplinary action.

5.3.6 General Computer Use – Personal Use and Privacy

Facilities: The Trust Network and ICT equipment is corporately owned and is primarily provided to support staff in their role for the benefit of our patients, staff and the business of the Trust The use of the Trust Network and ICT equipment for personal use is not forbidden, but is subject to adherence to the following principles and is a privilege that will be monitored and may be removed at any time. Personal use is expected to be kept to a reasonable level, during break periods and out of hours to avoid loss of productivity or distraction from primary tasks

Storage: Whilst the data storage facilities within the Trust Network are specifically for business purposes, the Trust acknowledges that staff may store a small amount of private and personal data within storage areas on occasions. Whilst the Trust will take every reasonable precaution to safeguard staff privacy, this cannot be guaranteed, and staff are advised to remove any personal data promptly. The Trust reserves the right to dispose of any such data, without prior notification, if it deems that the staff member is utilising a significant amount of space on the servers or it requires the space at short notice for business purposes.

Social Networking sites: This guidance is in addition to the procedures on e-mail and internet use and any relevant HR protocols. As staff are aware, the internet is provided primarily for business use. The Trust recognises that many staff use the internet for personal purposes and that many staff participate in social networking on websites; the purpose of this section is to specifically outline the responsibilities of staff using the internet to access social networking websites.

The Trust permits staff to access social networking sites on the Internet for personal use **only** before and after work hours and during a recognised lunch break. **Personal conduct:** The Trust respects an employee's right to a private life. However, the Trust must also ensure that confidentiality and its reputation are protected and, therefore, requires staff using social networking media to:

- Refrain from identifying themselves as working for the Trust.
- Ensure that they do not conduct themselves in a way that is detrimental to the Trust.
- Refrain from making disparaging comments or statements about the Trust, Trust employees, service users and their carers, Trust contractors and their agents.
- Take care not to allow any other interaction on these websites to damage working relationships between members of staff, service users and carers, contractors, partner or associated organisations and the general public.
- Refrain from posting any comment or media, displaying the user at work either undertaking work related activities or social activities with the exception of LPFT specific sites

Defamation: Any disparaging statement made by one person about another person or organisation, which is communicated or "published" may well be a defamatory statement and can give rise to an action for libel in English law.

Staff are advised that defamation can become a very serious issue and could result in legal proceedings. The Trust may take disciplinary action and/or civil action against defamation.
This applies to conduct and behaviour by individual staff both at work and outside of working hours away from the workplace, if it is likely to bring the Trust into disrepute or cause defamation

Monitoring of internet access at work: The Trust reserves the right to monitor staff internet usage at any time.
General monitoring may take place at any time by ICT technicians to ensure the operational functionality and data storage capacity of our network.
Targeted Monitoring such as checking an employee's internet usage may be due to suspicions that the employee has:

- Been spending an excessive amount of time viewing websites that are not work-related; and/or
- Acted in a way that damages the reputation of the Trust; and/or
- Acted in a way that breaches commercial confidentiality; and/or
- Breached this policy

The Trust reserves the right to retain information that it has gathered on staff use of the internet for an indefinite period.
The Trust reserves the right to restrict access to any websites at any time in the future and to monitor such use

Disciplinary action: If the Trust chooses to monitor staff internet use to ensure compliance with this policy, access to the Internet may be withdrawn in any case of misuse of this facility.
If a breach of this policy occurs, disciplinary action also is likely to be taken in line with the Trust's disciplinary policy

Security and identity theft: Staff should be aware that social networking websites are a public forum. Staff should not assume that their entries on any website will remain private. Staff should never send abusive or defamatory messages including attachments that may cause offence to others. Staff must be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, staff should ensure that no information is made available that could provide a person with unauthorised access to the Trust and/or any confidential information; and refrain from recording any confidential information regarding the Trust on any social networking website

5.3.7 Service user and Guest access

To preserve the confidentiality of all patients, staff and business information, without exception service users and guests are NOT permitted access to the Trust's network or ICT equipment that has access to Trust clinical and corporate systems.

Where the Trust wishes to provide fixed or wireless Internet access for service users and /or guests, hardware and software must be sourced through ICT services via a work package clearly stating the proposed use.

ICT services must configure this hardware and software to deny accidental access to the Trust's clinical and corporate systems.
It is most important that the Trust's communications cabinets or server rooms are NOT used to terminate ISP telephone or broadband lines. They should terminate near the service user's computer equipment completely separate from any Trust communication lines or equipment.

In some clinical areas Trust iPads **that are locked** to specific assessments or websites have been provided to support service user entry. These iPads are procured and set up by the ICT suppliers for the Trust; these do not connect to the Trust network but use a separate broadband connection or the cellular network. .

Service user computer equipment must be clearly marked "For Patient use – Do Not connect to the Trust's network"

Where teams or departments are providing Internet facilities for service users, they should organise the service through a commercial Internet Service Provider (ISP), such as BT or Virgin Media and this must be ordered through and supported by ICT services. Advice can be sought from the IM&T Development Manager in the Informatics Service on 01529 222330

5.3.8 Access to Personally Stored Corporate Electronic Data (CED)

Corporate Electronic Data (CED) is defined as:

a) All data, or information files, **created** on Trust computer software applications or computer systems
b) All data, or information files, **stored** on Trust computer hardware or networked systems or storage media
c) All data, or information files, **electronically communicated** through Trust's network systems including email and attachments

Staff are advised that all CED they produce during the course of their employment, remains the sole property of the employing organisation.

Computer networks provide the facility for sharing of CED which is essential to business activity. However the method and degree of CED sharing is governed by the 'need to know' principle, organisational policies and compliance with statutory legislation.

It is every staff member's responsibility to ensure that CED that needs to be shared is made available at the right time to the right person.
Line managers are responsible for ensuring that staff make CED available, where appropriate, in periods of planned or unplanned absence.

By exception, and to facilitate essential business continuity or for investigations into breaches of LPFT Policy to be undertaken, there may be a requirement for senior management to access CED which has been stored in staff's personal data areas or hard drives.

Strict guidelines must be followed to undertake this action that complies with The Regulation of Investigatory Powers Act 2000 (RIPA) and the rights and freedoms of individuals' under the Human Rights Act 1998.
In the event of accessing CED without the consent of the individual only the Chief Executive or an Executive Director may authorise this action.

The senior manager must complete a 'Request and Authorisation to Personally Stored Corporate Electronic Data (CED) form in full: http://icthelp.lincolnshire.nhs.uk/CED.htm

Once this form is countersigned by the Chief Executive or an Executive Director, it must be forwarded to the Deputy Director of Informatics or Head of Informatics, for them to action

The Chief Executive/Executive Director must ensure that the request is genuine and purposeful to maintain business continuity and be prepared to account for their personal actions to the Board, Court of Law or other legal body

Deputy Director of Informatics/Head of Informatics must only initiate the action on receipt of a fully completed request form. He/she must maintain the action log on the request form and ensure that the ICT service does not modify original files in any way (but can provide copies), and strictly enforces a policy of non-disclosure of user passwords.

5.3.9 ICT Asset Control

The Trust has a duty to protect its assets from loss or damage, to maintain equipment to a safe standard and to ensure the safe disposal of surplus equipment.

Pre Purchase Action

It is the responsibility of the designated budget holder to ensure that the following conditions have been satisfied before authorising the purchase of new or replacement equipment:

a) The accommodation and the proposed location for the new equipment is both adequate and appropriate and that where necessary advice has been sought from Informatics or the ICT department
b) There are sufficient electrical sockets available to service the new equipment, or that funding has been included in the costs for the installation of additional sockets (contact Estates for this function)
c) The need for the equipment is clearly identified and the most appropriate choice made on the request form
d) That all ICT equipment is purchased through the ICT department using the electronic ICT equipment ordering process which can be found here: http://sharon/lpft/PI/Pages/ICT-Equipment-Request.aspx

It is the responsibility of the approver of the ICT equipment request form to check:
a) The person ordering and the person approving the order is not the same person
b) The request is reasonable
c) That requests not perceived to be reasonable are escalated through the service line for review
d) That requests for new users are confirmed to be new users and that they are not replacement posts
e) Where replacement posts are identified that the local manager is prompted to follow asset register measures in paragraph 5.3.5
f) Where replacement/refresh ICT equipment is requested that a job has been first logged to the ICT service desk for review of the current kit and assessment for repair

All of these requests are expected to follow the electronic ICT equipment ordering process as above and will be subject to an authorisation review by the Head of Informatics and/or the Deputy Director of Informatics

It is the responsibility of the ICT department to ensure that the following considerations have been made:
- any maintenance requirements have been identified and agreed
- the disposal arrangements for the old equipment, including the potential cost, have been agreed
- equipment is marked with an asset number and included on the central inventory
- the order has followed LPFT ICT equipment ordering processes and ICT are in receipt of a valid order form

Purchase of assets at a cost greater than £5000

NHS England has set a capitalisation limit of £5,000. Therefore all tangible assets that are purchased for £5,000 or above must be included on the trust asset register, and be funded from capital resources

A tangible asset is something that will have an estimated life of greater than one year.

In certain circumstances, assets can be grouped to meet the £5,000 capitalisation limit. For this to be valid, the grouped assets must be functionally interdependent, under single managerial control, and each individual asset must have a value of over £500.

Advice as to whether a purchase should be funded from capital or revenue resources should be directed to the Finance department.

All purchases of capital assets must be approved by the Capital Steering Group.
All capital purchases must follow the Pre Purchase action as above in addition to including the asset on the Financial Asset Register. The ICT Capital budget is held by the Deputy Director of Informatics and any queries should be directed to them on 01529 222328

Condemning and disposing of assets

The ICT Service Delivery Manager is the nominated officer for the condemning of all ICT equipment owned by the Trust

Any item of equipment which is identified as damaged, broken, faulty or hazardous must be taken out of use immediately, labelled ‘Faulty do not use’ and securely stored until collection by ICT services

The ICT department must be notified immediately, detailing the fault and the location of the equipment

The ICT Service Delivery Manager or nominated deputy will assess the damage/fault and make the necessary arrangements for the safe disposal of any condemned equipment

The ICT department will ensure that the central asset register is updated

5.3.10 Email

Electronic mail (email) is accepted as one of the main working tools used on a daily basis. Most trust staff use email to send and receive messages, documents, appointments and tasks.

E-mail accounts are given to all LPFT employees as a business tool. However, although personal use of email facilities is discouraged they may, with discretion, be used for **limited** personal use provided that the content of messages is appropriate, i.e. is not likely to cause offence.
Employees should regard this facility as a privilege that is to be exercised in their own time without detriment to their job and with line management authority. This privilege is not to be abused. Employees are to be aware that

- The use of email, for both private and business purposes, will be monitored and therefore **privacy cannot be expected**
- Inappropriate or excessive use may result in disciplinary action and/or removal of facilities

Access to e-mail services as a business tools are **only** for legitimate communication, so called 'proper use'. Proper use is defined as information, which supports The Trust's clinical and operational activities and is sent only to those individuals who require the information to be transmitted.

Provision of e-mail services:

The provision of e-mail services will be managed centrally by AGEM CSU ICT Services.

Inappropriate Use of Email:

The use of e-mail in the following types of activities is specifically prohibited:

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with LPFT.
- Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitations of business or services, sales of personal property.
- Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes. Authorisation should be granted at team leader /service manager level.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files or communications belonging to others without appropriate authorisation or permission.
- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.
- The transmission of messages that may reasonably be considered offensive, lead to sexual or other types of harassment or cause personal distress.
- Giving opinions or otherwise making statements on behalf of the Trust unless appropriately authorised to do so.
- The transmission of messages that may reasonably be considered or interpreted as "bullying" in nature.

In addition the user must **NOT**:

- Attempt to use the e-mail system without having been assigned an authorised e-mail account.
- Make any attempt to infect other systems with a computer virus.
- Make any attempt to break into and/or access an e-mail account, which you have no legitimate right to use.
- Disclose their password to another individual.

These, and other inappropriate activities, may result in disciplinary action being taken against the person found misusing the e-mail service.

E-mail Etiquette

The Trust has a culture for using e-mail to communicate and therefore dealing with e-mail has become a full time job for many. There is therefore a need for staff to consider other routes of communication before using email, considering use of OCS, telephone, live meeting or speaking to another worker face-to-face. The following email tips are to help you when you are writing and responding to e-mails and it is encouraged for workers to challenge staff who are not following these tips. Lack of adherence to email etiquette will be monitored and action may be taken against repeat offenders.

1. **Don't assume people have received and read what you have sent**
   Just because you have sent an e-mail doesn't mean you have discharged your responsibilities. If it is important pick up the phone instead.

2. **Avoid "Me Too" and "Thanks" Messages**
   "Me too" is not enough content, but can cause annoyance. Also do you really need to send a reply of "Thanks" just to acknowledge that the email has been received?

3. **Do Not Default to "Reply All"**
   "Reply" is good. "Reply to All" is better; right? No. if you spent a bit of time composing and checking your e-mail you will probably find that most, if not all on the reply list, do not need to receive it.

4. **Always Check the Recipient of a Reply to a List Message**
   Don't send personal messages to millions. Double-check where you are sending your email, especially when you reply to a mailing list message.

5. **Check Other Replies Before Replying on a Mailing List**
   New ideas are better ideas. If you read all replies to a particular message on a mailing list before replying yourself, you can avoid repeating something that's already been said.

6. **Email Leaves a Permanent Record**
   Everything you mail is a written record and should be treated as such.

7. **Don't Forward Hoaxes, Jokes and Funny attachments – they may contain a virus**
   Email hoaxes often contain stories that are intriguing, jokes may be funny to some, attachments can be amusing to some but offensive and annoying to others. And worst of all they are used as a way of spreading viruses. Don't ever send them.

8. **Spell checking your e-mails automatically**
   Before hitting the send button spell check your e-mail. This can be done automatically.

9. **Request Return Receipts Sparingly**
   Do not always request a return receipt. Let recipients reply when/if they want.

10. **Keep Emails Short**
    Do not intimidate recipients with too much text. If it is more than a paragraph consider picking up the phone.

11. **Take Another Look Before You Send a Message**
    Don't send anything you don't want to send or to someone you don't want to receive it.

12. **What Can be Misunderstood Will be Misunderstood**
    The problem that whatever can be misinterpreted will indeed be misunderstood. Tone or intentions cannot be checked out with e-mail so be careful how you put things.

13. **Writing in All Caps is Like Shouting**
    Don't shout in your emails (and all capitals are so difficult to read).

14. **Think about why you are copying people in.**
    Don't copy people in for the sake of impact and affect. Copying senior people in or the individual's manager is not good practice and can create a negative view of you.

15. **Replying in anger is not good practice**
    If you are annoyed with the content of an e-mail you have received don't reply straight away. Take a break, make a cup of tea or do something else before you reply. You never know you may be misinterpreting the tone or the content.

16. **Email should have:**
    Subject line, Greeting, Body text, Sign off, Signature Block (contact details). Disclaimer.

17. **High Importance does not mean high priority**
    Just because you have clicked high priority doesn't mean it has the same priority for the person receiving it.

Priorities:

All routine messages are to be sent with the default (normal) importance tag set. The use of the High Importance tag is to be limited to urgent messages only. This is an important facility to help staff prioritise messages. The misuse of this facility may result in important messages being missed whilst less urgent messages are dealt with.

All e-mails containing confidential data **are** to be clearly marked by selecting the '**CONFIDENTIAL'** sensitivity from the option button on the toolbar. This facility can also be used to identify personal or private messages.

Signatures:

All users are to include a signature block to ensure that they are clearly identified. The signature block should be automated and is to include, as a minimum name, post, and address of the organisation and contact details. The signature block should also contain a confidentiality statement.

The Trust's recommended signature block is:

Forename and Surname
Post Title
Lincolnshire Partnership NHS Foundation Trust
Address
Tel: XXXXXXXXXXX Fax: XXXXXXXXXX Mobile: XXXXXXXXXX
CONFIDENTIALITY STATEMENT AND DISCLAIMER
This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Therefore if the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of the e-mail is strictly prohibited. Any views or opinions expressed are those of the author and do not necessarily represent the views of Lincolnshire Partnership NHS Foundation Trust unless otherwise explicitly stated. The information contained in this e-mail may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this e-mail and your reply cannot be guaranteed.

Practical use and house-keeping:

Care should be taken when sending file attachments as these are typically large and may cause network congestion. File attachments should only be sent when necessary and should be deleted as soon as is practicable.

Do not send e-mail with large file attachments (around **>250kb)** to multiple persons.
Do not send e-mail with very large attachments **(10Mb+)**. If this is necessary, advice should be sought from the ICT service desk.

All e-mail account or mailbox holders are responsible for the conduct and content of their mailbox. Never let anyone 'just use' your account, it is possible to formally share or delegate a selection of diary and e-mail functions while maintaining accountability.

The auto-forward feature of Microsoft Outlook **Must Never** be used to automatically forward mail to Non-NHS e-mail addresses. This specifically prohibits the use of personal Internet home accounts such as 'Hotmail' or 'AOL' for this purpose. The originator of a business message and the Trust has the right to assume that sending an e-mail to an NHS address should result in that e-mail terminating within the NHS environment, ideally at the formal location of the addressee or their deputy. Users who require access from external locations i.e. home are to request permission for remote access.

The amount of e-mail stored in a user's allocated personal storage area should be kept to a minimum. E-mails that need to be saved should be moved to a personal folder. Saved e-mails should be reviewed on a monthly basis and deleted when no longer required.

Storage: see Section 5.3.3 Data Security and Cyber Protection

Retention and Disposal:

Clinical: All clinical messages are to be either copied to an electronic clinical record or printed and stored in the paper health care record within 24 hours of receipt
Business: In accordance with the Freedom of Information Act records of business decisions taken by Trust employees, may be made available to members of the public on request. This includes decisions made by e-mail. Messages of this kind are to be kept for the duration of the project and either stored in an electronic folder (which pertains to the subject matter) or a hard copy should be taken and kept in the relevant file.

Personal: All personal messages **are** to be deleted as **soon as** they have been read.

Remaining Messages: All remaining messages are to be reviewed monthly and deleted if actioned.

Every member of staff has an obligation to report any actual or perceived inappropriate or unacceptable use of e-mail or the e-mail system, either through their line manager, via The Trust's Risk Management system or directly to the Information Governance Lead within the Informatics Service.

Cyber Security:

- Emails are one of the most vulnerable points of attack for an organisation. Inboxes are an easy point of access and offer a potential way into secure networks and systems. Up to 65% of emails can be spam and although firewalls are in place they cannot be the Trust's only line of defence. Some malicious emails are easy to spot, but others such as those mimicking a business email may compromise systems.
- As such it is vital that all Trust users are aware of the risk of, and identify and report suspicious emails to the IT service desk.

Confidentiality:

Trust e-mail is a secure method for the transfer of information within the local network which includes LPFT-LPFT email account, LPFT – LCHS email account, LPFT – Lincs CCG email account and LPFT – ULHT email account , and can contain patient identifiable or sensitive business information.

If you are unsure if the email account you are using, or sending to, falls into this jurisdiction then you must assume it is not secure and follow the following guidance.

The sender of an e-mail is responsible for the content, confidentiality and selection of correct delivery address of each e-mail.

The Trust approves NHSmail as a suitable method of transmitting sensitive or patient identifiable information in a safe and secure manner. All mail sent within NHSmail is encoded using robust ciphers for the duration of the transmission to the terminating mailbox where it is decoded for the addressee to read.

Additionally the Trust approves the use of NHSMail as a suitable method of transmitting sensitive or patient identifiable information in a safe and secure manner from an NHSMail account **to a non-accredited or non-secure email service** using the NHSMail encryption feature.

In an emergency, where speed clearly outweighs the risks, the responsibility for sending insecure e-mail to transmit PID or Corporate confidential data rests with the sender, who may subsequently be required to justify their actions.

Caution must also be exercised when sending e-mail to addresses external to the NHS. Each individual is responsible for risk assessing the decision to send any e-mail containing PID or confidential business information to a commercial or private e-mail address. The information should be fully encrypted.

Lincolnshire Partnership NHS Foundation Trust reserves the right to monitor its IT systems for the purpose of safeguarding staff by ensuring standards are maintained, conducting lawful investigations, ensuring the effective operation of systems and ensuring compliance with our statutory responsibilities. This monitoring will be carried out in accordance with the Information Commissioners guidance in this area and will comply with the Regulation of Investigatory Powers Act. The Trust will only permit the inspection, monitoring, or disclosure of e-mail, without the consent of the holder:

- When required by law.
- When there is reason to believe that Trust policies/legislation have been violated.

Automatic e-mail content filtering may be enabled to prevent inappropriate e-mail entering or leaving The Trust.

The Trust will endeavour to provide secure and reliable e-mail services. System Managers are expected to follow sound professional practices. However, since such professional practices and protections are not foolproof; the security and confidentiality of e-mail cannot be guaranteed.

All activity **must** comply with all relevant legislation, including the Data Protection Act 1998, Computer Misuse Act 1990, and the Caldicott recommendations.

All activity **must** comply with Trust Policies. All security breaches **must** be reported via the Trust's Risk Management system.

E-mail carries the same legal status as other written documents and should be used with the same care.

Exchanging Email with Service Users

The Trust recognises that there is a growing demand for communication with service users, carers and relatives using the e-mail facility. However as this method of communication could contain personal, clinical or sensitive information there are a number of thing which need to be considered and discussed with the data subject. Guidance is contained at Appendix A to assist staff with this.

5.3.11 EIS Access Control

This document:

- Sets out the organisation's process for the protection of clinical and corporate information systems by controlling access and availability.
- Establishes the responsibility for providing duly authorised access to and rescinding access from all Trust EIS.
- Authorises information system administrators/managers to undertake their duties**.**
- Applies to all staff, especially new starters, leavers and those changing job or responsibilities within the Trust.

An Electronic Information System (EIS) is defined as any multi-user computer system used to access, gather, process, and store information. Multi-user systems usually operate from a secure computer server room and are accessed from desktop or portable ICT equipment via a network. These systems may be exclusively owned, maintained and managed by the Trust, such as the Trust's network system itself, or by approved third parties under appropriate contract. An example is the IAPTus Clinical Records System, which is hosted in by a third party, Mayden. Appendix B contains a current list of the Trust's major EIS.

- Access to the Trust's EIS will be strictly controlled by formal registration and de-registration processes.

- The criteria for granting access to the Trust's EIS shall be based on business requirement and security. Each request for access shall be considered individually and should take account of security access levels, appropriate authorisation and strict application of the need to know principle.

- Physical access to Trust EIS equipment/server rooms will be strictly controlled and restricted to authorised personnel only using appropriate security and safety measures.

- To enable the segregation of duties and to enhance security, simultaneous and total, unrestricted access to all the Trust's EIS will not be permitted to any one member of staff at any time.

This document authorises the Administrators of the Electronic Information Systems listed in Appendix B to carry out their duties in accordance with the procedures agreed for each system.

For new workers the line manager must make all registration requests for both permanent and temporary staff, in writing to the appropriate System Administrator using the registration/de-registration procedure and form applicable to that system as follows.

A standard level of access, which should be clearly specified on request forms, will be granted on successful application. Other services will only be made available when specifically requested and authorised by Line Managers providing the access criteria are met.

Providing the appropriate procedures have been complied with, System Administrators should only grant EIS access after receipt of complete user registration requests. New user accounts may be set up in advance but not activated or made available, until the individual's actual start date and training has been provided by a clinical systems trainer or as otherwise agreed.

A unique user ID shall identify each user so that they can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out (i.e. Training).

Each EIS System Administrator/manager will maintain a record of all requests and file all original registration requests, both successful and unsuccessful, for verification or audit purposes.

For changes and amendments System Administrators should make the requested changes only after receipt of a properly completed request form, providing the appropriate procedures have been complied with and the access criteria met. System Administrators will keep a record of all change requests and file the original forms with all previous requests for that user.

Password format and general rules are set out in section 5.3.2.
Where a user has forgotten his/her password, the System Administrator or the helpdesk, for larger systems, is authorised to issue a replacement.
Upon receipt of such a request the System Administrator/Helpdesk will:

1. Ensure the request is logged.
2. Confirm the identity of the user
3. Issue a temporary, single use password, which should require, where established within the system, the user to change on first use.
4. Any potential or suspected security breaches must be reported on the LPFT Risk Management system.

Deregistration:

As soon as an individual leaves the Trust's employment, all their system logins must be revoked.

It is the responsibility of line managers to request user de-registration from ALL appropriate System Administrators as part of the employee termination process. The request should be made in advance of the users last day and specify a date and time for services to be revoked.

System Administrators should revoke user access rights at the requested time after receipt of a properly completed de-registration form. Old user ID's should be removed and not re-issued.

In an emergency any manager may request the ICT Service Delivery Manager or any System Administrator to immediately revoke a user's access. (Revoking network access may prevent access to other EIS). Providing the requesting manager can be positively identified, the requests must be actioned promptly by the System Administrator. The requesting manager must present completed de-registration form/s within one working day to the appropriate System Administrators and be prepared to justify his/her action.

System Administrators will keep a record of all de-registration requests and file the original forms with all previous requests for that user.

Privilege Management

"Special privileges" are those allowed to the system administrators or managers allowing global access to their systems for the purpose of performing their duties. This access may or may not include access to some or all data. The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached.

Privileged access must be authorised by the Director (or nominated Head of Department) responsible for each EIS and access forms completed as above. Audit processes will apply to all users including those with privileged access.

Review of User Access Rights

Each System Administrator or Manager should conduct a review of all access rights, to the network or EIS they are responsible for, at least twice a year. This action should positively confirm all current users. Any user accounts, which cannot be positively identified as current, must be disabled immediately, pending deletion. However, to allow for maternity leave or other extended absence, the System Administrator should check the status of users with their managers before deleting inactive accounts.

Network access:

Access to all Trust Electronic Information Systems (EIS) must commence with a formal written user registration request for Network Access, to AGEM ICT services. A separate user registration or change of requirements request must be made to each separate System Administrator controlling the access required to the any additional Electronic Information Systems required.

Access to the network should be made on the form available at the following link
http://icthelp.lincolnshire.nhs.uk/Access_Request_Form.htm

The function of remotely accessing the Trust's EIS from non-NHS sites is granted to fulfil business needs for flexible and mobile workers. Remote access uses the Pulse system and is a default setting on laptops. The provision of a laptop by a manager is also the authorisation for remote access. Further details can be obtained from the Deputy Director of Informatics or the Head of Informatics.

A separate user registration or change of requirements request must be made to each separate system with the System Administrator controlling the access required to the additional EIS required. Ultimate responsibility for systems access rests with the SIRO who is the Director of Finance and Information.

Access to RiO

Will be updated on system Go-Live

Access to Silverlink Mental Health System EPR

Procedures for access can be found here:
System procedures

Access request form:
User Access Registration and Deregistration forms
Authorised signatories:
Authorised signatories

Access to WebV Pathology system

Procedures for access can be found here:
System procedures

Access control matrix:
WebV Access controls matrix

Access request form:
User Access Registration and Deregistration forms
Authorised signatories:
Authorised signatories

Access to RBAC systems i.e. eReferrals and SystmOne

Procedures for access can be found here:
RBAC access

The guide for Smartcard users can be found at: users

Access to ESR

Procedures for access can be found here:

ESR Access Control guidance and User Access form

Access to E-Rostering

Process for access can be found here:

e-roster access form

Access to IAPTus

Procedures for access can be found here:
System Procedures

Access request form:
User Access Registration and Deregistration forms
Authorised signatories:
Authorised signatories

Access to SHARON

Procedures for access can be found here:

System procedures

Access to Integra/E-Series

Procedures for access and access request form can be found here:
http://sharon/lpft/Finance/Pages/Authorised-Signatories.aspx

If the system you require access to is not listed then please contact the System Manager or Administrator listed in Appendix B. If the system is not listed in Appendix B then contact the Head of Informatics at Trust HQ for further guidance.

Third party Users

Where there is a business need, strictly controlled third party access may be granted to the Trust's network infrastructure and processing facilities. Arrangements for third party access to the Trust's EIS should be based on formal contracts and service level agreements (SLA's), referring to all the security requirements to ensure compliance with the Trust's security policies and standards. Contracts and SLA's should ensure that there is no misunderstanding between the Trust and any third parties and comply with the requirements of ISO/IEC 17799:2000(E), paragraph 4.2.

Controlling both logical and physical third party access to Trust EIS, the ICT Security Lead should initiate a formally documented registration and de-registration process for each third party user. Before granting EIS access to third parties, approval must be obtained from the Head of Informatics, third party staff should be escorted and Trust IT staff should monitor all third party activity.

For further advice contact the Deputy Director of Informatics in the Informatics Service.

5.3.12 Mobile Phones

In this procedure the term mobile phone relates to any mobile phone procured by the Trust. Typically there are two types of phone:

- a Trust 'standard' phone
  This does not have data activation; this typically is a basic mobile phone model that does not have the necessary encryption to be permitted to use with Trust data; hence this will not be enabled even if the model would permit this
- a Trust 'smartphone'
  This is typically an Apple iPhone and does have the required encryption enabling use with all Trust systems (where systems are enabled for smartphone use) including access to MS Outlook and web browsing.

This procedure gives guidance to staff and managers on eligibility of provision of a work mobile phone, the requisitioning process and clarity relating to appropriate use of a work mobile phone including personal use.

This process outlines the legislation on the use of mobile phones in vehicles and other health and safety considerations. It also reinforces the mobile phone users' responsibility to ensure the security of personal identifiable data and to follow all guidance throughout this document.

This process further provides clarification on the appropriate use of mobile phones when contacting service users and carers.

Authorisation

The purchase and issue of mobile telephones is to be authorised for:

- Staff who work away from their base including lone workers

And/or

- Staff who are home-based

And/or

- Staff who need to be easily contactable during their normal working day due to the nature of their role

And/or

- Employees who are regularly on-call or on standby and need to be easily contactable outside of normal working hours

The Trust standard phone may be upgraded to a Trust standard Smartphone where:

- Staff require remote access to clinical data and a Smartphone is agreed to be the preferred route

And/or

- Staff who have VPN access and require remote access utilising the tethering function of the Smartphone

And/or

- Staff who are frequently away from an office base who require access to email on the move

And/or

- Staff who are flexible or home workers who, as part of their worker profile, require a Smartphone

Personal use:

The mobile telephone is, at all times the property of Lincolnshire Partnership NHS Foundation Trust (LPFT).

In general, mobile telephones will be provided by the Trust for work related purposes but can be approved for personal use by completing a request for personal use Template for Personal Use which is then approved by the Head of Service/Divisional Manager.

Personal usage means telephone calls/texts made (or accepted reverse charge calls) and data usage which is not wholly, exclusively and necessarily in the performance of the employer's duties. The monthly sum paid via salary sacrifice must cover all potential costs to the Trust but would not include overseas calls, donations by text, or charges by a third party. In these instances the Trust retains the right to recharge these additional charges to the individual.

Any personal usage must be reasonable and within the guidelines as stated above. Use of the phone for personal use in worktime must be kept to a minimum.

Personal smartphones must not be used for Trust business due to the device's ability to hold and store PID; the Trust does not currently subscribe to a Bring Your Own Device (BYOD) Policy. It is recognised however that staff may have their personal phones with them at work and all personal phone chargers used on Trust premises must be PAT tested in line with Trust policy.

Procurement:

All Mobile phones are to be ordered via the ICT department using the electronic form found at:
http://sharon/lpft/PI/Pages/ICT-Equipment-Request.aspx

The ICT department will purchase all LPFT's mobile phones using the current contract network provider and according to the LPFT phone catalogue/agreed tariff costs

The ICT department will purchase the mobile phone on the Trust's standard tariff for that device unless otherwise requested

The ICT department will monitor the use of mobile telephones using the network providers monthly call statement and recommend the amendment of any tariffs, as necessary, to the most appropriate for the level of call spend. They will inform the Head of Informatics who will liaise with the relevant budget manager.

The ICT department will monitor the use of mobile phones in respect of no charges incurred and after 3 months will call the number to check if in use. If no response this number will be disconnected. Services must ensure that within this 3 month period any phone required for business continuity purposes has a chargeable event made against it.

The ICT department will report any signs of suspected misuse to the Head of Informatics with regards to unusually high level of call spend; numbers utilised or extended call duration. The Head of Informatics will liaise with the relevant budget manager regarding action to be undertaken in line with this policy and procedure.

Clinical Use:

Text messaging is growing as a means of contact with service users between appointments and it is recognised that in certain services the use of mobile phones and text messaging is an essential way of communicating with service users. Managers should encourage appropriate use of mobile phones in these circumstances, but ensure that staff are aware of the risks.

- When texts are used a record must be made in the clinical notes of the time and date and content of the text, similarly a record must be made of any texts received from service users
- To minimise the risk of a service user needing urgent intervention and using text messaging as a means of getting this when it is more appropriate for them to speak to someone in person, or of a service user contacting a member of staff when they are on annual leave or on sick leave, service users need to be made aware that texting is only available during office hours and should sign a contract to say they understand how texts are to be used. Such a contract should specify that texts are only to be used when the member of staff is in work and arrangements for when the member of staff is on leave or off sick should be explicit within the contract. A copy of this contract should be kept in the clinical notes. Alternatively a mobile phone may be purchased for office use only to deliver/receive these texts which is then checked regularly throughout the working day by the office staff.

Mobile telephones issued by the Trust need only be switched on when the member of staff is on duty or on call. There is no expectation that staff have to remain contactable at any other time. Where staff use the same mobile for work and personal use they need to be aware of the implications of this when off duty or on leave i.e. if a service user or carer contacts them when off duty with a serious issue, therefore arrangements must be made with the local area line manager, on how to deal with calls that may be received outside of normal working hours.

Apart from the circumstances outlined above staff must be advised that they must not give their mobile telephone number to patients or carers. Patients or carers who may require advice or assistance should be encouraged to channel their request through the existing land line telephone systems. It is also possible to use the phone settings to withhold the telephone number.

Security, Loss or Damage:

The use of mobile phones must comply with PID guidance within the LPFT ICT Systems Use Policy and the NHS Information Governance guidance.

PID is information which can be identified to individuals and may thereby breach their right to privacy or present a risk of identity theft if lost or inappropriately shared. This applies to data relating to patients, staff and any other parties. It does not apply to identifiable data already in the public domain.

All mobile telephone PIN (personal identification number) codes must be enabled, with a complex password utilised on Smartphones.

The user should take all reasonable steps to prevent damage or loss to their mobile telephone. This includes not leaving it in view in unattended vehicles and storing it securely when not in use. The user may be responsible for any loss or damage if reasonable precautions are not taken.

All lost, stolen, or mislaid phones are to be immediately reported to the ICT Service Desk on **0300 1231020** for the telephone to be barred. (Delay in reporting could incur high costs to LPFT should the telephone fall into organised crime).

The user should inform their line manager of the loss and actions taken, and report the incident on the Trust Risk Management reporting system.

All requests for repair for mobile phones are to be directed to the AGEM CSU ICT Service Desk.

When a mobile phone is ready for disposal, it should be forwarded to AGEM CSU ICT Service Desk.

General Use:

All mobile phones are purchased with an international bar in place. To have the bar removed; authorisation from the relevant Divisional Manager or Head of Service must be passed to the ICT Department giving dates for the duration the bar is to be lifted. For longer or permanent removal of the international bar the CEO's permission must be obtained.

Safety and Driving:

The Trust will follow the current safety guidelines with regards to the operation of mobile telephones and will advise and amend its operational procedures to reflect changes in government advice.

If a member of staff is unhappy to utilise a Trust mobile telephone due to safety concerns there is no obligation to do so except for lone working reasons when it may be used on a hands-free basis.; however due to the potential risk to the worker of not having easy communication back to base this issue should be discussed with the line manager and recorded in supervision records.

Driving:

It is a specific offence to use a hand held phone or similar device when driving. Hands-free phones are also a distraction and individuals risk prosecution for not having proper control of a vehicle. The Trust advises that no mobile phones of any type, hand held or hands free, are used whilst driving and that the phone be switched to voice mail and the calls retrieved when it is safe and practical to stop the vehicle. However staff are permitted to use their own discretion in this matter so long as they remain within the boundaries of the law at all times.

Personal Mobile Phones – Privacy and Dignity

Mobile phones with the capability to take photographs and/or moving images represent a potential threat to the privacy and dignity of other staff, as well as service users, carers and relatives of service users. There is a potential risk of sexual harassment claims, as well as racial or disability discrimination and harassment. Under the rules of vicarious liability, the Trust could be held responsible for any discriminatory acts of its employees unless it takes reasonable steps to control them.

Accordingly, and via this procedure, the Trust advises staff that the use of such phones for taking video images and/or photographs is forbidden in the workplace without express consent. Any member of staff found to be taking photographs or video images of other staff or contractors, service users, relatives or carers without express consent may be subject to disciplinary action.

There are occasions where the use of a photograph can be extremely useful in helping to remedy, for example, equipment or building faults or damage. Providing care is taken not to breach the privacy or dignity of any individuals, the Trust may encourage such use, where to do so would expedite repairs or otherwise improve service delivery.

Personal mobile phone numbers must not be given out unless with the express permission of the individual.

Acceptable Use

All employees are expected to use Trust mobile phones in an appropriate and acceptable manner. The following are examples of what the trust feels is inappropriate usage and should be avoided (unless personal use is authorised and there is an arrangement in place to reimburse the Trust; see above) :

- Calls/texts to premium rate numbers e.g. 0800
- Calls/texts to votes of TV/radio programmes e.g. X Factor
- Calls/texts to betting/competitions
- Calls/texts to make donations
- Downloading of paid for apps (without written consent from a relevant budget holder)

The above list is not exhaustive and other examples could be considered by senior managers as inappropriate.

5.3.13 Staff Activity Audit and Investigations

In support of an existing investigation or to support a manager with a reasonable suspicion of a breach of Trust policy or working practice, the Trust will initiate investigations into staff computer system activity, both internal and external, including current and past email and Internet activity, and their use of any part of the Trust's ICT network and systems.

Investigations may include targeted monitoring of any past and present staff activity using ICT including phone systems, examination of electronic records and journals and the seizure of Trust equipment for examination.

Investigation into inappropriate access to patient data

The line manager for the individual suspected of using Trust Information Systems for unauthorised activity contacts the Data Protection Officer (DPO) and follows the procedure outline in the LPFT Systems Access Investigation Procedure

Investigation into staff computer system activity

Each investigation must be authorised by a Trust Director and be fully documented. Investigating officers and managers who require an ICT systems investigation should follow the outlined process in procedure 5.3.8 and provide:
a. Full details of the staff member and the equipment they use
b. Justification criteria
c. The period of the investigation or the start and end dates
d. Additional information about existing investigations and the location of any equipment.

In all circumstances requesting Officers are encouraged to contact the Data Protection Officer, Head of Informatics or the Deputy Director of Informatics to discuss their concerns, determine if an investigation is viable and to seek assistance as required.

Routine audit of sensitive records i.e. staff records will be undertaken; the process for this can be found here: http://sharon/lpft/Clinical/General%20Trust%20Wide%20Documents/Access-Forms-Clinical-Systems/EIS%20Policy%20documents/Process%20for%20auditing%20access%20to%20electronic%20records%20(2).docx

6. Implementation

Action	Timeframe
Email sent to Divisional Managers/ Clinical Directors and Heads of Service informing them of the amended policy and requesting dissemination through their staffing structure.	Within a week of policy approval
Status of new Policy advertised through the Trust's Weekly Word and an announcement placed on the Informatics SHARON site	Within a week of policy approval, repeated weekly for four weeks
Policy uploaded to Trust website with active links to access from both Internet and Intranet sites	Within a week of policy approval
Clinical systems and IT skills training sessions to highlight existence of Policy	To incorporate within lesson plans within one month of policy approval

7. Monitoring

Standard	Measurables	Lead	Frequency	Reporting To	Action Plan/ Monitoring
The provision of the Trust's ICT systems will be managed and maintained centrally by the Trust's ICT supplier under SLA	Number of incidents of provision of ICT services being provided by an external supplier (not agreed with ICT services)	ICT Service Delivery Manager	Bi-annually	IM&T Committee	Action Plan: Relevant Lead in conjunction with IM&T committee colleagues. Monitoring: IM&T Committee
Inappropriate incidents of access to the Internet.	Number of inappropriate incidents of access to the Internet	Deputy Director of Informatics	Bi-annually	IM&T Committee	Action Plan: Relevant Lead in conjunction with IM&T committee colleagues Monitoring: IM&T Committee
Access is provided to the N3/HSCN through a secure gateway, and the Trust's Wide Area Network management will be in accordance with the NHS Statement of	Number of breaches of the Trusts SOC Confirmation that a secure firewall is in	Deputy Director of Informatics ICT Service Delivery	Bi-annually Bi-annually	IM&T Committee IM&T Committee	Action Plan: Relevant Lead in conjunction with IM&T committee colleagues. Monitoring: IM&T Committee Action Plan: Relevant Lead in conjunction

Compliance. The Trust operates a secure Firewall between the Trust's Local Area Network and N3/HSCN.	place at all times during the last monitoring period	Manager			with IM&T committee colleagues. Monitoring: IM&T Committee
Virus protection: ICT will ensure that appropriate technical steps are taken to reduce the vulnerability of the LPFT network to attack from computer viruses.	Number of incidents of breach of virus protection	ICT Service Delivery Manager	Bi-annually	IM&T Committee	Action Plan: Relevant Lead in conjunction with IM&T committee colleagues. Monitoring: IM&T Committee
Access to the Trust's computer system is only permitted to authorised staff that have completed the registration process, obtained their own unique personal username and password, and if appropriate received training.	Number of incidents of unauthorised access to Trust computer systems broken down by type	Head of Informatics	Bi-annually	IM&T Committee	Action Plan: Relevant Lead in conjunction with IM&T committee colleagues. Monitoring: IM&T Committee

8. Associated Documentation

Appendix A: Guidance for Agreeing an E-mail Exchange with a Service User.
Appendix B: Lincolnshire Partnership NHS Foundation Trust Managed EIS
Appendix C: e-Rostering Procedure

Guidance for Agreeing an E-mail Exchange with a Service User.

When a requirement for an email facility has been established, a clinician should meet with the service user to explain the email facility and answer any questions. It is most important that the following two points are specifically explained:

- The service user should be cautioned to take care compiling their messages to NHS staff as email carries the same weight in law as the written word and the authority of the sender.

- E-mail should not be used for urgent messages, such as reporting a crisis. In situations where contact needs to be made urgently, service users and carers should be advised to use an alternate direct method, such as a landline.

Once the service user is clear on the preceeding two points, the benefits and the risks associated with sending personal information over email should be explained and advice offered on how best to use the service and mitigate the risks.

Benefits:

1. Fast and direct communication. Email is very fast and normally delivers messages within 10 minutes, however this does assume that the recipient is available to check their mailbox at regular intervals.

2. Email can be sent and read at any time, though it will only be dealt with during normal office hours and according to staff availability. Received email will sit in the recipient's inbox until they choose to read them.

Risks:

1. The security of email cannot be guaranteed by the Trust in respect of the service users commercial mailbox account. Once outside the NHS system, email should be considered insecure and the service user must accept responsibility for the security and privacy of the email from that point.

2. Service users need to be aware that if they share their computer or passwords with family members, partners or housemates, they may also be sharing the personal information contained in their email. Therefore, they should be advised to take the appropriate precautions, such as securing any information they wish to keep private or disposing of this appropriately.

3. When a service user chooses to use this email facility their informed or explicit consent must be obtained and recorded along with their email address as a prerequisite to initiating the information exchange process.

To help mitigate the risks and follow best practice, both Service Users and NHS staff should:

1. Only send the minimum amount of personal or clinical information required.

2. Be aware that emails carry the same weight in law as the written word. Therefore, service users should not allow anyone else to send email on their behalf to the NHS team, unless by prior arrangement, and take care wording email.

3. Always ensure the email is correctly addressed, before sending.

4. Ensure received email is read and acted upon promptly.

5. Once viewed and actioned email should be printed and filed on the paper health record or where in use scanned into the electronic patient record.

Service Users Consent

When a service user chooses to use the email facility, after the benefits, risks and mitigating actions have been fully explained, it is good practice to obtain and record their written informed consent.

Staff should be aware that while this consent does not indemnify the Trust, in any way, it does highlight our responsibility to ensure that all relevant information is provided and fully explained to the service user.

A suggested example of a consent form follows, which should be tailored to suit the department's requirements and circumstances:

Service Users E-mail Consent

I have been made aware or the benefits and risks of using email to exchange personal information and authorise:

Staff Member ……..

Team ……

Organisation ……

to use my email address to inform or advise me in relation to my current care plan/course of treatment.

Service User's Signature ……..…..

Full Name (Print) ……. NHS Number ……

Email Address ……

Date ……

Appendix B

Lincolnshire Partnership NHS Foundation Trust Managed EIS

System Name	System Type	Access Type	IAO	Contact
Trust ICT Network	Network access to Trust EIS & applications, Local and NHS Intranet and the World Wide Web.	General network access to personal and shared storage, Trust & NHS e-mail, local office applications - controlled by username and password	Local Managers for shared drives and local applications See IG lead for specific IAAs	Fen House 01522 563070
Electronic Staff Record	Workforce Development System	Role based access managed through Smartcard	Head of Workforce and Development	Trust Headquarters 01529 222262
Integra General Ledger	Corporate Financial System	Locally managed multi-user system controlled by role specific access via username and password	Head of Procurement	Gervas House 01522 464478
Lease Cars	Corporate Financial System	Appointed single user access only	Head of Payroll and Pensions	Gervas House 01522 546546
DATIX	Risk Management Reporting System	Profile based access via username and password	Head of Informatics	Trust Headquarters 01529 222328
SharePoint	Document Management system	Locally managed multi user system controlled access via user name and password	Systems Manager	Trust Headquarters 01529 222328
Role Based Access Control	NHS England Care Records Service	Secure controlled access by Smart-Card Chip & Pin in conjunction with Job Role & Business Function	Registration Authority Manager	Cross O'Cliff Court 01522 513355
Silverlink Mental Health System	Electronic Patient Record	Role based access controlled by username and password	Head of Informatics	Trust Headquarters 01529 222328
IAPTus	Electronic Patient Record	Role based access controlled by username and password	Head of Informatics	Trust Headquarters 01529 222328
eReferrals	Electronic Patient Referral system	Role based access managed through Smartcard	Head of Informatics	Trust Headquarters 01529 222328
RiO	Electronic Patient Record	Role based access managed through Smartcard	Head of Informatics	Trust Headquarters 01529 222328
SystmOne	Electronic Patient Record	Role based access managed through Smartcard	Head of Informatics	Trust Headquarters 01529 222328
WebV	Pathology Results system	Locally managed access via username and password	Head of Informatics	Trust Headquarters 01529 222328
ePEX	Electronic Patient Record – access to archived data	Locally managed access via username and password Within Clinical Systems only	Head of Informatics	Trust Headquarters 01529 222328

Appendix C

E-ROSTERING PROCEDURE

http://sharon/lpft/Clinical/General%20Trust%20Wide%20Documents/Access-Forms-Clinical-Systems/EIS%20Policy%20documents/FINAL%20DRAFT%20E-Rostering-Policy.docx

Lincolnshire Partnership NHS
NHS Foundation Trust

GENERIC EQUALITY IMPACT ASSESSMENT TEMPLATE

INITIAL EQUALITY IMPACT ASSESSMENT

STAGE 1 - Screening to establish if the proposed function has any relevance to any equality issue and/or minority group			
Directorate: **Finance**	**Function to be Assessed:** **ICT Systems Use Policy v4.0**	**Existing or New Function:** **Existing function**	**Assessment Date:** **01/06/2018**

1. Briefly describe the aims, objectives and purpose of the function:			Providing an ICT systems use management framework to preserve confidentiality, integrity and availability of information across all Trust ICT systems and users in LPFT	
2. Who is intended to benefit from this function, and in what way?			Staff, management, third parties, partner agencies and temporary staff by setting standards for security of Trust ICT systems.	
3. What outcomes are wanted from this function?			Staff compliance with relevant legislation. Understanding of the principles of computer use and how these will be implemented ensuring a consistent approach to security and behaviour creating an awareness of the need for computer security, the risk of cyber-attack and of protecting information assets.	
4. What factors/forces could/ contribute/ detract from these outcomes?			Lack of training for staff. Failure of staff to implement standards. Lack of awareness of risk.	
5. Who are the main stakeholders in relation to the function?			All staff. Executive team and Board of Directors. IM&T Committees, system users and line managers.	
6. Who implements the function, and who is responsible?			Everyone working in the NHS has responsibilities to adhere to the standards in this policy. Chief Executive has ultimate responsibility; SIRO has Trust Board level accountability.	
7. Are there concerns that the function has a differential impact on the following groups and what existing evidence (either presumed or otherwise) do you have for this?				
Race		**N**	Please explain:	
Disability		**N**	Please explain:	
Age		**N**	Please explain:	
Gender		**N**	Please explain:	
Religion or Belief		**N**	Please explain:	
Sexuality		**N**	Please explain:	
If the answer to question 7 is 'YES', a partial EIA must be completed. Should the function proceed to a partial impact assessment?				**N**

If no, please state date of next review: 01/06/2020 Date on which partial impact assessment to be completed by:

I understand the Impact assessment of this function is a statutory obligation and that, as owners of this function, we take responsibility for the completion and quality of this process.

Signed (Assessor).....Date…01/06/2018.....

Print Name.....Carolyn Holmes.....

Signed (Section Head) Date.....

Print Name.....