East Lancashire Hospitals NHS Trust TRUST WIDE DOCUMENT	
Delete as appropriate	**Policy**
DOCUMENT TITLE:	Information Security Policy
DOCUMENT NUMBER:	**ELHT/C045 Version 3.3**
DOCUMENT REPLACES Which Version	ELHT/C045 Version 3.2, ELHT c047 v3.1, ELHT C111 ver 1.1, ELHT C046 ver 4.1, ELHT C102 ver 2, ELHT C121 ver 1.1 and ELHT C044 ver 2
LEAD EXECUTIVE DIRECTOR DGM	Director of Finance Planning and Information
AUTHOR(S):Note should not include names	Head of ICT

TARGET AUDIENCE:	All Trust Personnel
DOCUMENT PURPOSE:	To safeguard the security of the Trust's information assets by ensuring availability and preserving integrity and confidentially.
To be read in conjunction with (identify which internal documents)	

SUPPORTING REFERENCES	• BS ISO/IEC 27001:2013 • ISO TR 21730:2007 • Information Governance Toolkit

CONSULTATION		
	Committee/Group	**Date**
Consultation	Information Governance Steering Group (IGSC)	16/01/2018
Approval Committee	Information Governance Steering Group (IGSC)	16/01/2018
Ratification date at Policy Council:	V1 May 2005 V2 November 2008 V2.1 January 2012 V2.2 January 2013 V2.3 July 2015 V3 April 2016 V3.1 August 2017 V3.2 March 2018 V3.3 October 2018	
NEXT REVIEW DATE:	October 2021	
AMENDMENTS:		

Table of Contents

1. Introduction

This policy manual defines the Information Security Policies for East Lancashire Hospitals NHS Trust.

The Information Security Policies apply to all business functions within the scope of the Information Security Management System (ISMS), and covers the information, information systems, networks, physical environment and relevant people who support those business functions.

This manual sets out the organisation's policies for the protection of the confidentiality, integrity and availability of the hardware, software and information handled by information systems, networks and applications. It also establishes the security responsibilities for information security and provides reference to the documentation which comprises the ISMS for the above scope.

This policy also brings together and consolidates the following policies into one document; ELHT/C0045 Version 2.3,- Information security Policy, ELHT c047 v3.1, - Pc Policy, ELHT C111 ver 1.1,- I.T Systems Access Policy, ELHT C046 ver 4.1, - Internet Email Policy, ELHT C102 ver 2, - Mobile Devices Policy, ELHT C121 ver 1.1 – I.T asset Management policy, ELHT C044 ver 2 – IM&T Disaster Recovery Policy

2. Objective

The objective of this policy is to safeguard the security of the Trust's information assets by ensuring availability and preserving integrity and confidentiality

3. Scope of this Manual

This manual covers all information systems, networks, applications, locations and people within the ISMS for the major business processes carried out by the Trust.

4. Manual Overview

East Lancashire Hospitals NHS Trust information systems, applications and networks are available when needed, they can be accessed only by legitimate users and contain complete and accurate information. The information systems, applications and networks must also be able to withstand or recover from threats to their availability, integrity and confidentiality.

To satisfy this, East Lancashire Hospitals NHS Trust will undertake to the following: East Lancashire Hospitals NHS Trust will:

- Protect all hardware, software and information assets under its control. This will

be achieved through the implementation of a set of well-balanced technical and non-technical measures

- Provide both effective and cost-effective protection that is commensurate with the risks to its assets
- Implement the Information Security Policies in a consistent, timely and cost effective manner

East Lancashire Hospitals NHS Trust will comply with laws and legislation including:

- Common Law, that is, ensure that normal civil responsibilities apply
- Freedom of Information Act
- Computer Misuse Act
- Copyright, Designs and Patents Act
- Data Protection Act
- EU Privacy and Electronic Communications Directive
- The Human Rights Act 1998 (article 8);
- The Freedom of Information Act 2000;
- The Data Protection Act 1998 including S.29;
- The Common Law Duty of Confidence.

East Lancashire Hospitals NHS Trust will carry out security risk assessment(s) in relation to all the business process covered within this manual. These risk assessments will cover all information systems, applications, PCs and mobile end user devices and networks that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Formal risk assessment will be conducted to determine the Information Technology Security Evaluation Criteria (ITSEC) Assurance levels required for security barriers that protect the information systems.

System Security Procedures for all information systems, applications and networks will be produced. These procedures will be developed on the basis of an analysis of risks. These must be approved by the Information Security Manager (ISM) both at the beginning of the project and prior to the implementation of any information system.

Security Operating Procedures and security contingency plans that reflect System Security Policies will be produced. All users of the system must be made aware of the contents and implications of relevant System Security Policies and Operating Procedures.

The Trust will ensure that a key part of any project deliverable will be an understanding and written undertaking that responsibility for producing and implementing effective security countermeasures, producing all relevant security documentation, security operating procedures and contingency plans reflecting the

requirements of the System Security Policy are set out in the project/programme plan.

The Trust will ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action(s).

The Trust will ensure that all information systems, applications and networks are approved by the Information Security Manager (ISM) before they commence operation. In this role the Information Security Manager will be supported by the Information Technology Security Officer (ITSO). The ITSO is responsible for ensuring that the information systems do not pose an unacceptable security risk to the organisation. The ITSO will also provide written progress reports and updates for the Information Governance Steering Group.

The ISM and/or the ITSO may require checks on, or an audit of, actual implementations based on approved security policies.

The Trust will ensure that measures are in place to detect and protect information systems, applications and networks from viruses and other malicious software.

The Trust will ensure that changes to the security of an information system, application or network are reviewed by the relevant project/system manager. All such changes must be reviewed and approved by the ITSO. The project/system managers are responsible for updating all relevant System Security Policies, design documentation and security operating procedures. The ISM and/or the ITSO may require checks on, or an assessment of the actual implementation based on changes implemented.

The Trust will ensure that all connections to external networks and systems have documented and approved System Security Policies. The ITSO must approve all connections to external networks and systems before they commence operation. The Trust will ensure that all operational applications, systems and networks are monitored for potential security breaches. All potential security breaches must be investigated and reported to the ITSO. Security incidents must be reported in accordance with the requirements of the organisation's incident reporting scheme.

The Trust will ensure that there is an effective configuration management system for all information systems, applications and networks.

5. Security Responsibilities

5.1 Overall Responsibilities

The Chief Executive as Accountable Officer has delegated the overall security responsibility for security, policy and implementation to the Information Security Manager (ISM).

Responsibility for implementing this policy within the context of IT systems development and use in the organisation is delegated further to the Information Technology Security Officer (ITSO).

5.2 Head of Organisation's Responsibilities

The Chief Executive is responsible for (but may delegate this duty to the Senior Information Risk Owner(SIRO)) for :

- Making arrangements for information security by setting an overall information security policy for the organisation
- Appointing the Information Security Manager
- Appointing an officer to ensure that the provision of the Data Protection Act is satisfied
- Ensuring that, where appropriate, staff receive IT security awareness and training

5.3 Information Security Manager's Responsibilities

The Information Security Manager is responsible for:

- Participating in the Information Governance Steering Group.
- Reporting to the Information Governance Steering Group on matters relating to IT security.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Representing the organisation on internal and external committees that relate to IT security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally by the Information Security Manager.
- Ensuring that access to the organisation's assets is limited to those who have the necessary authority and clearance.
- Providing advice and guidance to development teams to ensure that the policy is complied with.
- Approving system security policies for the infrastructure and common services.
- Approving tested systems and agreeing rollout plans.
- Advising the Information Security Manager on the accreditation of IT systems, applications and networks.
- Providing a central point of contact on IT security issues.
- Providing advice and guidance on:
  - Policy Compliance
  - Incident Investigation

- IT Security Awareness
- IT Security Training
- IT Systems Accreditation
- Security of External Service Provision
- Contingency Planning for IT systems

- Contacting the Information Security Manager when:
  - Incidents or alerts have been reported that may affect the organisation's systems, applications or networks.
  - Proposals have been made to connect the organisation's systems, applications or networks to systems, applications or networks that are operated by external organisations.
- Passing on the advice of external sources/authorities on IT security matters.

5.4 Data Protection Officer's Responsibilities

The Data Protection Officer is responsible for:

- Ensuring that appropriate Data Protection Act notifications are maintained for applicable organisation's systems and information.
- Dealing with enquires, from any source, in relation to the Data Protection Act and facilitating Subject Access Requests.
- Advising users of information systems, applications and networks on their responsibilities under the Data Protection Act, including Subject Access.
- Advising the ICO on breaches of the Act and the recommended actions.
- Encouraging, monitoring and checking compliance with the Data Protection Act.
- Liaising with external organisations on Data Protection Act matters.
- Promoting awareness and providing guidance and advice on the Data Protection Act as it applies within the organisation.

5.5 Line Manager's Responsibilities

Line Managers are directly responsible for:

- Ensuring the security of the organisation's assets, that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Ensuring that their staff are aware of their security responsibilities.
- Ensuring that their staff have had suitable security training.
- The Information Security Sub Group of the E-Health Programme Board is responsible for ensuring security and data protection is considered when applications and systems are under development or enhancement. In the absence of a Project Board the responsibility for security falls to a nominated Project Officer. The development of a security policy for the application or system should commence at the preparation phase of any project or programme.

5.6 General Responsibilities

All personnel or agents acting for the organisation have a duty to: Safeguard hardware, software and information in their care.

- Prevent the introduction of malicious software on the organisation's IT systems.
- Report on any suspected or actual breaches in security.

6. Guidelines

See Information Security Policies – Detailed Guidelines Appendix B. Additionally detailed advice on how to determine and implement an appropriate level of security is available from the Information Security Manager (ISM) and Information Technology Security Officer (ITSO).

6.1 Validity of this Policy/Manual

This policy should be reviewed annually under the authority of the Information Security Manager. Associated information security standards should be subject to an on-going development and review programme.

Appendix A: Named Officers

Chief Executive
Mr Kevin McGee Chief Executive East Lancashire Hospitals NHS Trust Royal Blackburn Hospital Blackburn BB2 3HH

Senior Information Risk Officer
Mr Jonathan Wood Director of Finance, Information and Planning East Lancashire Hospitals NHS Trust Royal Blackburn Hospital Blackburn BB2 3HH

Information Security Manager (ISM)
Miss Debbie Wilson Head of Information & Communication Technology East Lancashire Hospitals NHS Trust Royal Blackburn Hospital Blackburn BB2 3HH

Data Protection Officer
Mr Salim Badat Head of informatics Business Support and Interim Information Governance Manager East Lancashire Hospitals NHS Trust Royal Blackburn Hospital Blackburn BB2 3HH

Appendix B: Information Security Policies

B1 Purpose

The purpose of this appendix is to present all the Trust IT security policies procedural information and guidance in a single location.

B2 Background

In 2001 the NHS IM&T Security Manual was replaced by British Standard BS7799 as a guide to good information security practice in the NHS. The British Standard controls and objectives are aligned with those listed in the International standards BS ISO/IEC 27002:2005. This standard has since been superseded by BS ISO/IEC 27002:2013. This document has adopted the guide line and recommendation laid out in BS ISO/IEC 27002:2013 as a best practice.

The Trust is required to complete and submit the NHS HSCIC Information Governance Toolkit on an annual basis, the purpose of which is to provide assurance the Trust is applying appropriate security standards across all its business practices.

B3 Risk Management and Compliance

ELHT will use Risk Management procedures to estimate threat probability including the security risks to information systems; their vulnerability to damage, and impact of any damage caused. Measures will be taken to ensure that each system is secured to an appropriate and cost effective level and that data protection principles are implemented.

Risk Assessments will be conducted with regard to every system and will assess compliance with relevant security policies procedures; ensures good working practices are being maintained and review security breaches. Assessments will take place regularly and are the responsibility of each system manager (Information Asset Assistant) and Information Asset Owner. Assessments will include:

- Identification of assets and threats such as fire, flood, machine failure, operator error, or malicious interference for example, hacking or burglary)
- Evaluation of the impact of an adverse event or threat on the assets
- Assessment of the likelihood of the threat occurring
- Identification of practical, cost effective counter measures to protect the asset and/or limit the damage caused by an event
- Formal report to the IT Services and Strategy Manager for improved information security performance (and then to the Information security Sub Group for review and recommendation on actions)
- Monitoring of risk will be integrated with the incident reporting process.

1.0 Security Responsibilities

1.1 Definition

At top level, the Chief Executive, Director of Finance and the Associate Director of Performance & Informatics have responsibility for Information Security. At a practical level the following responsibilities are in place:

- Information Asset owner – Each information asset will have a nominated person who is accountable for the asset. Assets may be grouped for ease of management.
- Systems Manager (Information Asset Assistant) – each information system will have a nominated person who will be accountable for all the information assets comprising the system.
- The Head of ICT – IT services will be accountable for the IT infrastructure (including all Computer Rooms, data communications closets and data network), hardware assets. Within IT Services security responsibilities apply to the assets, processes and activities in the areas as follows:
  - Networks Manager - Data network
  - Infrastructure Manager – Computer Rooms assets,
  - Desktop Support Manager – PCs, notebook PCs and peripherals.
- Caldicott Guardian
- Data Protection Officer

1.2 Security Awareness

Recruitment procedures and awareness initiatives will include reference to information security and the need to protect patient privacy. Users will be aware of information security responsibility to reduce risk of human error, theft, fraud or misuse of facilities.

- Staff will be notified of the Confidentiality Agreement within each Contract of Employment and informed of the need to adhere to the Information Security Policy and the Data Protection Policy.
- Confidentiality agreements, reference to Information Security and data protection will be incorporated into employment contracts with agencies providing temporary, contracted staff e.g. PFI. Other contract staff will be required to sign an agreement to abide by the same codes of conduct and discipline as permanent staff.
- Where appropriate job descriptions should reference responsibility for Information Security. An outline of roles and responsibilities will include general responsibilities for implementing or maintaining information security policy as well as specific responsibility for the protection of assets or for particular security processes or activities.
- Security minded recruitment procedures will also include
  - Interview, provision and checking of references
  - Confirmation that individuals are not engaged in activities which might lead to a conflict of interest

- The contract, job description and New Starter Induction process will raise user awareness of information security and Data Protection Policy and induction/ starter packages should ensure users are equipped to support security policy in the course of their work.
- The Information Security Policy and associated Detailed Guidelines will be published and otherwise made available to all employees.

2.0 Information Sensitivity Classification

2.1 Reasons for Classification

To assist in the appropriate handling of information, a sensitivity classification hierarchy must be used throughout all NHS Organisations. This hierarchy provides a shorthand way of referring to sensitivity, and can be used to simplify IT decisions and minimize IT costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, where it goes, or who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories

2.2 NHS Confidential

This should be used for patients' clinical records, patient identifiable clinical information, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies. This will include patient demographic details that might identify people who have had a GP contact/hospital appointment within a particular timeframe or who may have a particular condition. (**NOTE**: In order to safeguard confidentiality, the term "NHS Confidential" should **never** be used on correspondence to a patient)

3.0 Legal Obligations and Related Policies

The Trust will comply with this policy in conjunction with current legal obligations and EU directives to maintain information security and confidentiality; with any other legal and common law obligations and with best practice policies and statements of the NHS.

The Trust will avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations and of any information security requirements.

3.1 Intellectual Property Rights

- Legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products will be complied with.
- The intellectual property rights over any software developed by the trust or by staff on behalf of a Trust will be the property of the Trust and therefore Crown Copyright.

- Should the Trust contract with a software development company to produce a software application, then the intellectual property rights of the resulting software should be considered and agreed at the outset and included in the contract.

3.2 There is a common law obligation for staff to preserve the confidentiality of information.

3.3 Relevant legislation, existing NHS policies and existing ELHT policies must be complied with.

3.4 Procedures will be implemented to ensure compliance with the Data Protection Principles, and:

- The Trust will appoint a Data Protection Officer responsible for providing guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed.
- All users, managers and system managers have a responsibility to prevent unlawful disclosures of personal information.
- The Trust is registered under the Data Protection Act for relevant purposes and the details of this registration are reviewed annually.
- Information assets will only be used for the purpose for which they were intended.

3.5 System specific contracts and service level agreements will be complied with.

3.6 Access to systems will be authorised and controlled.

3.7 Access to and use of cryptography will be controlled in accordance with legal requirements, HSCIC guidance and with Trust policy.

3.8 Evidence required against a person or organisation within the Trust, will be collected in accordance with any published standard or code of practice for the production of admissible evidence.

4.0 Enabling the Flow of Information

4.1 Patient Identifiable Information

The Trust is fully committed to the Caldicott Principles regarding the protection and use of person identifiable information, namely;

- Use and transfer of such information will only take place where absolutely necessary and the purpose is fully justified;
- The number of data items that could allow identification of an individual must be reduced to the minimum essential for the purpose. Where possible all data should be anonymised;
- Access will be strictly “need to know” and in accordance with the guidance in “The Protection and Use of Patient Information”. Access will be

reviewed every three years;

- Everyone must understand their responsibilities and comply with the law;
- Person identifiable information must not be shared with unauthorised persons.

4.2 Sharing data/information with partner organisations.

The Trust works with partner organisations which all have a legitimate role to play in delivering care to NHS patients. Partners, in this context, are taken to be:

- Social services;
- Education Services;
- District Councils
- Other Local Authority Services
- Voluntary Sector providers;
- Independent Sector providers;
- Independent GP Practices
- Independent Pharmacists, Opticians and Dentists
- Private Finance Initiative providers

Formal information sharing protocols will be developed, which will make the standards of information protection control explicit rather than implicit.

4.3 Sharing data with non-partner organisations

In addition to partner organisations, the ELHT organisations receive regular requests for person-identifiable information. Organisations requesting such information include:

- Police
- Insurance companies
- Solicitors

Whilst such requests may be legitimate, ELHT will ensure the use of such information is not abused. For further information Ref: Data Protection Policy.

4.4 Privacy Impact Assessments (PIA)

Privacy risk assessments/ privacy impact assessment (PIA) are an effective way to demonstrate how any potential privacy data threats and the likelihood of them happening were reduced at the start of a project/ programme or planned change to a service

It is mandated that a PIA should be used:-

- When reviewing, planning or redesigning changes to an existing information system.
- The introduction of a new system, a new information asset or the initiating of a new project which involves the use of personal data.
- When modifying existing programs or activities where personal information is being used, or intended to be used, in a decision-making process that directly affects an individual or group.

- When personal data is intended to be used or shared in a decision making process which will directly affect an individual.
- Contracts out or transfers a program or service to another level of government or the private sector resulting in substantial modifications to a program or activity.
- A data sharing initiative between two or more organisations which proposes to pool data together.
- A new database which consolidates information held by separate organisations.
- New legislation that impacts on the privacy through the collection of data, or through surveillance or other monitoring formats.

5.0 Surveillance

Surveillance can be undertaken only with the consent of the proper authorities and in accordance with law. Covert surveillance (both intrusive and directed) as defined under the RIP Act will not be carried out by the Trust. In the event of suspected fraud or breaches of criminal law, the appropriate authorities will be consulted.

IT SHOULD BE NOTED that routinely all actions carried out by Trust staff when using IT equipment and systems is logged. This information may be viewed when investigating suspicions of abuse and may be used as evidence in disciplinary procedures.

6.0 Private Work

The following conditions apply to use of Trust IT equipment and services for personal purposes: -

- IT equipment and services are provided primarily for use for Trust purposes. Management may authorise limited personal use as a benefit to staff, provided this does not interfere with the performance of their duties.
- Use of IT equipment and services for private work resulting in personal commercial gain is not permitted.
- When using IT equipment and services for private work, the tenets of the PC Policy and of the Internet and Email Policy apply and must be complied with by the user.
- The user must comply with the Information Security Policy of this organisation. In particular, if taking equipment off-site, the user must comply with the rules for Off-site (and home) Working outlined in this policy.
- No information or software should be loaded which would compromise the use of equipment for work purposes.
- No software should be attempted to be loaded onto trust equipment without express permission from IT Services.
- Information intended to be processed for personal purposes, which is covered under the Data Protection Act, must NOT be stored on Trust equipment.

7.0 Printing, Copying and Fax Transmission

7.1 Destruction of Waste Copies

Individuals are responsible for ensuring that all copies of sensitive information are removed from printers, copiers and fax machines and the associated print queues. All paper copies of sensitive information must be disposed of in a secure waste container approved by the Trust.

7.2 Faxing Precautions

Materials classified as NHS Confidential must not be faxed unless an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site, the fax is sent to a secure room to which only the authorized staff have access, or a password-protected fax mailbox is used to restrict release to an authorized recipient. NHS Confidential information must not be faxed through untrusted intermediaries such as hotel staff or rented mailbox.

8.0 Storage of information outside the corporate infrastructure

Storage of information classified as NHS Confidential is prohibited on data storage systems hosted outside of the Trusts infrastructure unless approval by Information Governance. This includes cloud-based hosted services such as DropBox, SkyDrive etc.

9.0 User Anonymity

Staff must not misrepresent, obscure, suppress or replace their own or another member of staff's identity on the Internet or on any other Trust/NHS information system. In all instances, the user ID, email address, organisational affiliation, and related contact information must reflect the actual originator of a message or posting. The use of anonymous re-mailers of other identity-hiding mechanisms is forbidden.

10.0 System Vulnerability

All staff in receipt of information about system vulnerabilities must forward this information to the Information Security Manager, who will determine what action is appropriate. Staff must not redistribute system vulnerability information.

B4 Internet, email and instant messaging

UPDATED DECEMBER 2017

1. Who this policy applies to

1.1. All users of Trust information systems

2. This policy should be read alongside:

2.1. Access control policy
2.2. Mobile device policy

3. Introduction

3.1. Communications play an essential role in the conduct of our organisation. The Trust values your ability to communicate with colleagues, patients and business contacts and invests substantially in information technology and communications systems which enable you to work more efficiently and effectively and expects you to use these facilities responsibly
3.2. How you communicate with people not only reflects on you as an individual but on the Trust as an organisation. Therefore, although we will respect your personal autonomy and privacy, we have established this policy which lets you know what we expect from you and what you can expect from us in your use of email, instant messaging and internet access
3.3. We expect you to use the information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties, with respect for your colleagues and in accordance with the Trust's policies and procedures
3.4. Any inappropriate use of the Trust's communications systems whether under this policy or otherwise may lead to action being taken against you under the Trust's disciplinary procedures

4. The Trust's commitment

4.1. Appropriate equipment and systems will be provided to enable staff to make best business use of electronic communications systems
4.2. Backup, recovery and archive facilities will be available
4.3. The default applications in use are Microsoft Outlook, Microsoft Lync or Skype and Microsoft Internet Explorer (or IE)
4.4. Basic instruction will be made available to cover the use of email, messaging and internet access to those users who require it
4.5. Secure methods of transfering confidential and sensitive information will be provided. This may include the use of NHS.net mail or encrypting the source data
4.6. All traffic transmitted via email, internet or instant messages may be monitored
4.7. Mechanisms will be provided to protect the Trust's information systems from attack by computer viruses, worms and other malware
4.8. Access to certain websites is blocked. If you have a particular need to access such sites, please apply by logging this request with the ICT service desk. Access will only be permitted for Trust purposes
4.9. A disclaimer will be automatically added to all external mail sent from the Trust

4.10. Although these facilities are intended to be used for business purposes, we appreciate that you may occasionally wish to use the system and/or the facilities for your own purposes. This is allowed as long as you comply with the requirements of this policy. Be aware that if you choose to make use of Trust facilities for personal correspondence, you can expect very little privacy because the Trust may need to monitor communications

4.11. The Trust accepts no responsibility for any losses you may suffer as a result of personal use

5. Your commitment

5.1. You must:

5.1.1. Ensure that you are logged onto the network using your personal username and password before making use of internet access, email or instant messaging

5.1.2. Keep your personal passwords private – do not disclose them to anyone

5.1.3. Change your passwords from time to time for security purposes – if you suspect any other person knows your password you MUST change it immediately

5.1.4. Ensure that your usage falls in line with local departmental arrangements

5.1.5. Only use Trust provided email, messaging and internet facilities and NHS.net mail for authorised purposes

5.1.6. Ensure that any personal use of internet, email and instant messaging facilities:

5.1.6.1. Does not interfere with the performance of your duties

5.1.6.2. Does not take priority over your work responsibilities

5.1.6.3. Is minimal and limited to taking place in your own time

5.1.6.4. Does not incur unwarranted expense or liability on the Trust

5.1.6.5. Does not have a negative impact on the Trust in any way

5.1.6.6. Does not cause disruption to the Trust's data network – personal use is best restricted to times outside the normal working day and the transmission of large files is discouraged (anything over 5MB in size)

5.1.6.7. Is lawful and complies with this policy

5.1.7. Ensure that personal emails contain the text 'Personal' in the email subject line so that personal emails may be identified as such. If an email message does not contain this text then the message will be assumed to be a business communication

5.1.8. As a manager, log any concerns over the abuse of personal use with the ICT service desk where it will be treated confidentially and investigated by a senior member of ICT

5.1.9. Exercise due care when collecting, processing, storing or disclosing any personal data and only process personal data on behalf of the Trust where it is necessary for your duties

5.1.10. Take care when using these methods as a means of communication as all expressions of fact, intention and opinion via email may bind you and/or the Trust and can be produced in court in the same way as oral or written statements

5.1.11. Be aware that once you have sent an email you have no control over it. This means it may be read by people other than those who you intended

5.1.12. Comply with the relevant legislation, which includes:

5.1.12.1. Data Protection Act

5.1.12.2. Freedom of Information Act

5.1.12.3. Regulation of Investigating Powers Act

5.1.12.4. EU Privacy and Electronic Communications Directive

5.1.12.5. Computer Misuse Act

5.1.12.6. Copyright, Designs and Patent Act

5.1.13. Manage the content of your email folders proactively including checking the amount of space used and deleting messages no longer required

5.1.14. Comply with any enforced quotas

5.1.15. Follow email etiquette: (note that these principles should also be used when making use of instant messaging facilities)

5.1.15.1. Be sure to check your 'Inbox' regularly

5.1.15.2. Always include a 'Subject' header line

5.1.15.3. Ensure you only send or copy emails to recipients who should receive the email

5.1.15.4. Never send an 'angry' email

5.1.15.5. Avoid attachments if you can. The use of 'cut and paste' is generally much more efficient both in time and storage space

5.1.15.6. Don't include graphics unless necessary. Picture files tend to be large and take up a lot of bandwidth and storage space

5.1.15.7. **Before** hitting the 'send' button always:

5.1.15.7.1. Double check that the list of recipients (including CC and BCC) is correct

5.1.15.7.2. That any attachments are in fact attached

5.1.15.7.3. That you have used the spelling checker tool and corrected errors

5.1.15.7.4. Reread to ensure the content is not inappropriate in any way

5.1.15.7.5. Note that the use of 'recall' is generally unsuccessful

5.1.15.8. Do not type all of your message in capitals.

5.1.15.9. When forwarding emails include the reason for forwarding in the subject line of the message and the body of the text.

5.1.15.10. Use 'Out of Office Assistant' when you are absent for a period of time.

5.1.15.11. Only certain staff are able to send All-User emails. If you have a message which you wish to send to everyone, the correct procedure is to ask your Director's Secretary/PA in the first instance

5.1.15.12. On all matters relating to email and internet security, rely on the ICT. They are the only people who should inform users of security risks. Even if you are requested to do so, do not pass on such messages (e.g. virus warnings) to other users – the request may be a hoax

5.1.15.13. Managers have a responsibility to plan for the continued processing of emails after an employee leaves. It is recommended that the Helpdesk is informed prior to the leaving date so that the appropriate arrangements can be agreed and put in place.

5.1.15.14. Make use of the 'Signature' facility within Outlook to set up your name, title, phone number, etc., together with a disclaimer.

5.1.16. Only use approved connection methods to access the internet from Trust equipment

5.1.17. Ensure that all material which is received from any external source or downloaded from the Internet (e.g. as email attachments), is checked for malicious code

5.1.18. Ensure that you are aware of Freedom of Information and Data Protection guidelines. Remember that any retained data may have to be disclosed in legal proceedings or in response to a request under the Data Protection Act or Freedom of Information Act. The golden rule is therefore never to write anything which would embarrass you or the Trust if it became public

5.2. You must not:

5.2.1. You must not use another persons ID or password to access any Trust system

5.2.2. Access any other person's in-box or other e-mail folders or send any e-mail purporting to come from another person except where specifically authorised by the other person

5.2.3. Amend any messages received

5.2.4. Rely on email as an instant communication method if the e-mail message or attachment contains information which is time-critical

5.2.5. Release any confidential information via these methods without authorisation. All information relating to our patients and our business operations is confidential

5.2.6. Send confidential or sensitive information via these methods as they are unlikely to be secure. If in doubt – ask for advice from ICT

5.2.7. Send or forward any messages that are abusive, defamatory, offensive, obscene or malicious.

5.2.8. Make improper or discriminatory reference to a person's race, colour, religion, gender, age, religion, national origin, disability or physique or make derogatory or offensive comments

5.2.9. Send any containing information which may be perceived as damaging to the reputation of the Trust

5.2.10. Use the internet, email or messaging for purposes which would violate local statues, laws or regulation, inclusive but not limited to; duplication or dissemination of personal identifiable information, patient and staff records

5.2.11. Display of any kind of sexually explicit or racist or offensive image or document on any Trust system

5.2.12. Archive, store, distribute, edit or record sexually explicit, racist or offensive material using the Trust's network or computing resources

5.2.13. Breach copyright or trademark law

5.2.14. Visit sites that are deemed inappropriate categories. Attempt to access these types of sites will be monitored and reported to HR and Line Managers

5.2.14.1. Adult/Sexually Explicit

5.2.14.2. Criminal Activity

5.2.14.3. Gambling/Online Auctions/Pay to Surf

5.2.14.4. Games

5.2.14.5. Hacking
5.2.14.6. Alcohol/Illegal drugs
5.2.14.7. Intimate Apparel & Swimwear
5.2.14.8. Intolerance & Hate
5.2.14.9. Peer-to-Peer files sharing sites
5.2.14.10. Personals & Dating
5.2.14.11. Phishing, Fraud and Theft
5.2.14.12. Ringtone/Mobile Phone Downloads
5.2.14.13. Spam URLS
5.2.14.14. Spyware
5.2.14.15. Tasteless & Offensive
5.2.14.16. Violence
5.2.14.17. Weapons
5.2.14.18. Web based email or chat
5.2.14.19. Streaming Media
5.2.14.20. Use of unauthorised Remote Access Tools
5.2.14.21. Proxy Avoidance

5.2.15. Use any Trust system in connection with the operation of management of any other business or for commercial transactions, advertisements or promotions

5.2.16. Use Trust accounts such as your email address when using public websites for non-business purposes, such as online shopping, booking holidays, banking etc

5.2.17. Introduce any unauthorised software to the Trust's systems. In particular you should not open any attachments with an .exe extension or open any attachments which appear to be programs

5.2.18. Introduce any form of spyware, computer virus or similar malware

5.2.19. Carry out any kind of hacking activities

5.2.20. Circumvent any mechanisms provided to protect the Trust's information systems from attack by computer viruses, worms and other malware

5.2.21. Maliciously tamper with any computer system in an attempt to disable, defeat or circumvent any security systems put in place to monitor and control activities on the internet

5.2.22. Use the system in any way which may damage, overload or affect the performance of the system or the internal or external network

5.2.23. Independently arrange internet access direct with any commercial internet service provider

5.2.24. Use commercial web-based email services such as Hotmail, Outlook, Gmail, Yahoo mail, and the like

5.2.25. Connect any Trust equipment to the internet via a modem and phone line

5.2.26. Store any information on your local PC

5.2.27. Store information on Trust computer equipment that is of a non-business nature

6. Suspect emails

Email is frequently used to deliver unwanted material, which is at best, annoying, and at worst, malicious and can cause considerable harm to your computer and yourself. These can come in a number of forms

6.1. Spam or Junk email
  6.1.1. Examples include:
    6.1.1.1. Advertising, for example online pharmacies, pornography, dating, gambling
    6.1.1.2. Get rich quick and work from home schemes
    6.1.1.3. Hoax virus warnings
    6.1.1.4. Hoax charity appeals
    6.1.1.5. Chain emails which encourage you to forward them to multiple contacts (often to bring 'good luck').
  6.1.2. How to spot spam – they may feature some of the following warning signs:
    6.1.2.1. You don't know the sender
    6.1.2.2. Contains misspellings (for example 'p0rn' with a zero) designed to fool spam filters
    6.1.2.3. Makes an offer that seems too good to be true
    6.1.2.4. The subject line and contents do not match
    6.1.2.5. Contains an urgent offer end date (for example "Buy now and get 50% off")
    6.1.2.6. Contains a request to forward an email to multiple people, and may offer money for doing so
    6.1.2.7. Contains a virus warning
    6.1.2.8. Contains attachments, which could include .exe file
  6.1.3. The risks:
    6.1.3.1. It can contain viruses and spyware
    6.1.3.2. It can be a vehicle for online fraud, such as phishing
    6.1.3.3. Unwanted email can contain offensive images
    6.1.3.4. Manual filtering and deleting is very time-consuming
    6.1.3.5. It takes up space in your inbox

6.2. Scam email – usually delivered as a spam email, but try to trick you into disclosing information that may lead to defrauding you or stealing your identity
  6.2.1. Examples include:
    6.2.1.1. Emails offering financial, physical or emotional benefits, which are in reality linked to a wide variety of frauds
    6.2.1.2. These include emails posing as being from 'trusted' sources such as your bank, HMRC or anywhere else that you have an online account. They ask you to click on a link and then disclose personal information.

6.3. Phishing email
  6.3.1. Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually try to trick you into going to the site, for example to update your password to avoid your account being suspended. The embedded link in the email itself goes to a website that

looks exactly like the real thing but is actually a fake designed to trick victims into entering personal information.

6.3.2. The email itself can also look as if it comes from a genuine source. They may even contain your name and address. Fake emails sometimes display some of the following characteristics, but as fraudsters become smarter and use new technology, the emails may have none of these characteristics.

6.3.2.1. The sender's email address may be different from the trusted organisation's website address

6.3.2.2. The email may be sent from a completely different address or a free webmail address

6.3.2.3. The email may not use your proper name, but a non-specific greeting such as "Dear customer."

6.3.2.4. A sense of urgency; for example the threat that unless you act immediately your account may be closed

6.3.2.5. A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website

6.3.2.6. A request for personal information such as username, password or bank details

6.3.2.7. The email contains spelling and grammatical errors

6.3.2.8. You weren't expecting to get an email from the organisation that appears to have sent it

6.3.2.9. The entire text of the email may be contained within an image rather than the usual text format.

6.3.2.10. The image contains an embedded link to a bogus site

6.4. Some tips to help you to use email safely:

6.4.1. You must:

6.4.1.1. Be suspicious of all emails received – it is very easy to forge or spoof and email

6.4.1.2. Report any suspicious or malicious emails it to the ICT service desk immediately i.e. virus, spyware, fraudulent, phishing etc

6.4.1.3. Delete any suspicious emails once reported to ICT

6.4.1.4. Report to the ICT service desk if you have opened a suspicious email, attachment, clicked on a suspicious link or suspect that your device may be infected with a virus

6.4.1.5. When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails

6.4.1.6. Delete all addresses of previous parties in the email string, before forwarding or replying

6.4.1.7. Unplug your network cable, turn off wireless or power down your computer if you suspect your computer has become infected with a virus or malware. Report the suspected infection immediately to the ICT service desk

6.4.1.8. Take notice of all advice being publish by ICT – all security bulletins from ICT will be published in a standard format

6.4.2. You must not:

6.4.2.1. Open emails which you suspect to be suspicious

6.4.2.2. Forward emails which you suspect to be suspicious, even if you are requested to do so (expect from requests by ICT)

6.4.2.3. Reply to any unwanted email – including using 'Reply all'

6.4.2.4. Open attachments unless it is from a trusted source and you are expecting it

6.4.2.5. Click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email

6.4.2.6. Respond to emails from unknown sources

6.4.2.7. Click on 'remove' to remove yourself from the email subscription

6.4.2.8. Disable any mechanisms which have been implemented to protect the Trust's information systems from attack by computer viruses, worms or other malware

Remember –

1. These methods may also be used to target users via other methods of communication such as by traditional post or telephone. The Trust has previously had malicious phone calls from someone posing as the ICT helpdesk asking users to give remote access to computer devices
2. If you aren't sure about something – check it out
3. Be vigilant when receiving or responding to emails
4. Review it, report it and delete it

B5 Use of Mobile Devices

UPDATED AUGUST 2018

1. Who this policy applies to

1.1. All users of mobile phones

2. This policy should be read alongside:

2.1. Mobile phone policy
2.2. Mobile working policy

3. Introduction

3.1. Communication with family and friends is important when someone is in hospital or receiving health care
3.2. Overly-restrictive policies may act as obstacles to beneficial technology and may not address the growing need for personal communication of patients, visitors and the workforce. At the other extreme, unmanaged use of mobile communications can place patients at risk
3.3. The use of mobile devices should be allowed within Trust sites as long as this does not present a threat to the safety of patients, the operation of medical devices or peoples privacy and dignity
3.4. Mobile devices include laptops, notebooks, portable storage, gaming, mobile and tablet devices – anything that is enabled with wireless network capabilities
3.5. The 'use' of mobile phones within this policy is deemed to include the use of that device for the purpose of sending or receiving voice calls, SMS (text) messaging, e-mails and all other data transfer

4. The Trust's commitment

4.1. The Trust will actively manage the use of the radio frequency spectrum across its sites in line with MHRA recommendations. This includes considering areas where medical devices will not be affected and therefore no restrictions apply and other areas where authorised staff can use communication devices authorised by the hospital
4.2. The Trust will report incidents to the MHRA when a medical device is suspected to have suffered electromagnetic interference
4.3. There are 3 categories of mobile phone areas across the Trust:
  4.3.1. Category 1 – Non Clinical areas/low risk patient areas (e.g. clinic waiting areas, corridors, reception areas), where mobile phones can be used by staff, patients and visitors alike
  4.3.2. Category 2 – Clinical Patient areas (e.g. general wards, departments, patient homes) where mobile phones can be used by staff, patients and visitors, but may be subject to local restrictions if their use is deemed to be affecting patient care, dignity or confidentiality
  4.3.3. Category 3 – Safety Critical Patient areas (e.g. Intensive Care/NICU/Theatres) Mobile phones must be switched off in these areas
4.4. Patients and visitors must switch phones to vibrate/silent in category 2 areas, if they wish to talk after 10pm or before 7am they must find a local category 1 area e.g. corridor

4.5. Staff, patients and visitors will be made aware of the areas within the Trust where the use of mobile phones is restricted or limited through the use of signage
4.6. The Trust will not take responsibility for patient's and visitor's mobile devices whilst they are on Trust property
4.7. The use of camera phones may compromise patient confidentiality. The Maternity units may permit photos to be taken with a mobile phone, for example, parents with their new-born baby as long as no staff or other patients are in the photo
4.8. Certain exemptions will be allowed where mobile devices can be used:
4.8.1. When senior on-call clinicians and managers may need to be urgently contacted whilst in a patient area
4.8.2. Where there is a clinical imperative that negates the use of all other means of communication
4.8.3. Where there is an urgent need for translation at the bedside of a patient and no advocate is available to attend
4.8.4. A Major incident has been declared
4.8.5. Staff who meet the criteria for a temporary exemption to the policy are politely asked to show consideration to the enforcement of the policy to colleagues, patients and visitors. It is accepted that it is the circumstances at the time that dictate the clinical imperative and as such people who are using their phones are requested to give consideration to politeness and professionalism

5. Your commitment

5.1. You must:
5.1.1. Take responsibility for your own mobile devices whilst on Trust property
5.1.2. Keep any personal mobiles device on silent, unless working in a Category 3 area where they must be switched off. The only exemption being the staff member needs their phone on them for Trust business (e.g. consultant on call). Staff should not have their phones on them whilst in the clinical areas, they should be kept with other personal items e.g. handbag, backpack etc
5.1.3. Be mindful of moderation of tone, volume and language when using mobile devices on Trust premises
5.1.4. Place personal mobile devices on silent and not accept any calls when you are visiting clients/patients/service users in their own home
5.1.5. Only charge mobile devices using an official (not generic) phone charger that has been Portable Appliance Tested (PAT). Only spare power sockets can be used with an understanding that other devices will take priority where limited sockets are available. Mobile phone chargers will also have to be unplugged when not in use
5.1.6. Ensure that patients and visitors to the Trust are made aware of this policy and the implications of none compliance – which includes being asked to leave or calling security
5.1.7. Inform patients and visitors if their behaviour is deemed disruptive – they must be mindful of moderation of tone, volume and language with respect to use of communication devices. Telephone ringing and subsequent conversations may disrupt important patient/ healthcare

professional activities or may disturb and/or alarm patients who are resting

5.1.8. Ensure that any use of photo or video applications to take images or recordings of staff or patients has the consent of the staff or patient concerned

5.1.9. Advise patients who are leaving the ward to use their phone that mobile devices should NOT be used within 1m of active infusion pumps and monitors

5.2. You must not:

5.2.1. Use mobile devices within two meters of any medical equipment. Even when such devices are on standby, they emit a signal

5.2.2. Use loud ring tones or alarms on personal or Trust supplied mobile phones as these may be confused with alarms on medical equipment

5.2.3. Use integral cameras/ document management functions within any form of personal mobile communication device for clinical purposes

5.2.4. Use a handheld mobile device whilst driving on Trust business. It is an offence under the Road Traffic Act to use a handheld mobile device whilst driving

5.2.5. Allow patients or visitors to charge their mobile devices when on Trust property

6. MHRA recommendations

The MHRA recommendations for use of mobile communications devices are outlined below for information.

RISK OF INTERFERENCE	TYPE OF COMMUNICATION SYSTEM	RECOMMENDATION
High	Analogue emergency service radios.	Use in hospitals only in an emergency, never for routine communication.
	Private business radios (PBRs) and PMR446. E.g. porters' and maintenance staff radios (two-way radios).	Minimise risks by changing to alternative lower risk technologies
Medium	Cell phones (mobile phones). TETRA (Terrestrial Trunked Radio System). Laptop computers, palmtops and gaming devices fitted with higher power wireless networks such as GPRS* and 3G. HIPERLAN**.	A total ban on these systems is not required and is impossible to enforce effectively. Should be switched off near critical care or life support medical equipment. Should be used only in designated areas. Authorised health and social care staff and external service personnel should always comply with local rules regarding use
Low	Cordless telephones (including DECT***). Low power computer wireless networks such as RLAN**** systems and Bluetooth	These systems are very unlikely to cause interference under most circumstances and need not be restricted.

B6 Mobile Devices

UPDATED DECEMBER 2017

1. Who this policy applies to

1.1. All users of mobile devices

2. This policy should be read alongside:

2.1. Mobile phone policy
2.2. Mobile working policy
2.3. Password policy
2.4. Email and internet policy
2.5. Patching policy

3. Introduction

3.1. Mobile devices enable you to access information on the move facilitating more flexible working practices
3.2. However, they also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the Trust's data and ICT infrastructure. This can lead to data leakage and system infection
3.3. We must protect our information assets in order to safeguard our patients, data and reputation. We must therefore ensure that mobile devices are used in a safe and secure environment
3.4. Mobile devices include Trust supplied laptops, notebooks, portable storage, mobile phones – with or without a data allowance and tablet devices – including iPads. They will be configured to have access to corporate networks, data and systems
3.5. The Trust will supply and manage all mobile devices – BYOD (bring your own device) is **not** supported
3.6. All mobile devices across the Trust must be procured through ICT
3.7. All applications for mobile devices must have the support of the budget holder
3.8. Users who are authorised to have a Trust mobile device configured to access email will not be eligible to be configured for OWA (Outlook Web Access)

4. The Trust's commitment

4.1. Trust mobile devices will be:
4.1.1. Configured with appropriate software including security software and apps
4.1.2. Updated to use the latest operating system in line with the Trust's patching policy
4.1.3. Configured with software to prevent access to inappropriate web pages. This includes pornography and illegal sites as well as gambling and discriminatory sites
4.1.4. Configured to access Trust email accounts
4.1.5. Configured to access the appropriate Trust information systems
4.1.6. Secured with appropriate PINs, passcodes or passwords in line with the Trust's password policy

4.1.7. Supplied with a charger and optionally a protective case and additional keyboard
4.1.8. Managed and secured via the chosen Mobile Device Management (MDM) security solution
4.1.9. Supplied with 3G or higher mobile access dependant on user needs
4.1.10. Barred from international roaming unless there are exceptional circumstances where business use overseas is deemed unavoidable
4.1.11. Enabled for access to the Trust's corporate wireless network if the device has data capabilities. The device will default to this on Trust premises where the wireless network is available

4.2. All mobile devices will remain the property of the Trust at all times
4.3. Initial training and ongoing support will be provided by ICT
4.4. ICT will supply and manage all mobile devices requested and approved through the approval process available on the ICT Service Desk
4.5. Software updates will be managed using the MDM security solution
4.6. All Trust mobile devices will be registered as an asset on the IM&T asset management system and will be associated to the main user
4.7. The device location can be tracked by ICT
4.8. All mobile devices will be blocked and remotely wiped upon notification of loss or damage by the user
4.9. The Trust will provide a single network provider for all applicable Trust supplied mobile devices. Currently the supplier is BT – formally EE, Orange and T-Mobile
4.10. Other network providers are available on a case-by-case basis. An alternative provider is usually selected where there are issues of coverage with the Trust's provider of choice. All instance of variance from the provider of choice must be signed off by the Director of Finance
4.11. A bill management solution will be available to enable budget holders to have visibility of costs and usage of mobile devices charged to their budgets
4.12. The usage of mobile devices will be reviewed on a monthly basis using the bill management solution and unusual/unexpected/unexplained usage will be investigated
4.13. Personal use of Trust mobile devices is allowed as long as this is declared and such use falls within the agreed policies and working practices. Any associated costs will be deducted from salaries
4.14. Personal use of Trust mobile devices will be monitored to ensure that it does not impact on working practices
4.15. Where applicable, budget information will be transferred to East Lancashire Financial Services (ELFS) for the management of recharges, credits and deductions from salaries
4.16. All devices will be reviewed by ICT on an annual basis to determine suitability and usage

5. Your commitment

5.1. You must:
5.1.1. Complete your application for any mobile device through the ICT Service Desk which includes consideration of your eligibly for such a device
5.1.2. Ensure that you have authorisation from the budget holder before you make your request and include a relevant budget code as part of the

application. This will cover the costs of the device and any monthly charges as well as software licenses including those for MDM and email usage

5.1.3. Be aware of Trust rules relating to the personal use of email, internet and intranet facilities

5.1.4. Declare any personal use of Trust provided mobile devices so that appropriate deductions can be made from salaries. Misuse of mobile devices will lead to disciplinary action being taken against you in accordance with the Trust's disciplinary policy

5.1.5. Accept updates to the mobile device which are published by ICT

5.1.6. Keep the mobile device in any protective case if one is supplied to minimise the possibility of damage

5.1.7. Ensure that the mobile device is charged at all times during working hours

5.1.8. Take care of your mobile devices and ensure that they are safe and secure at all times to ensure the risk of theft is minimised. For example, ensure that mobile devices are locked when unattended, do not leave a mobile device in your car overnight and take extra care when using mobile devices in public places

5.1.9. Alert ICT immediately if it is suspected that unauthorised access to information has taken place via a mobile device in line with the Trust's incident management policy

5.1.10. Alert ICT immediately upon discovery that a mobile device or associated equipment is lost, stolen or damaged. This includes using the ICT out of hours service if applicable.

5.1.11. Be responsible for any replacement or repair charges for equipment that is lost or damaged

5.1.12. Notify ICT if the device is no longer required, is being transferred to another user or if you are changing roles but plan to retain the device

5.1.13. Ensure that all mobile devices are returned before you leave the employ of the Trust. Charges for outstanding mobile devices may be made

5.2. You must not:

5.2.1. Delete any of the tablet software installed by the Trust. This software is essential to keep the device secure

5.2.2. Modify the mobile device in any way

5.2.3. Install any other software or applications onto the mobile device

5.2.4. Remove the SIM card if there is one installed

5.2.5. Disable the PIN, password, passcode, fingerprint identity sensor or any other security feature

5.2.6. Use your mobile device whilst driving or in restricted areas

5.2.7. Use the mobile device in any way that could bring the Trust into disrepute

5.2.8. Openly work with sensitive information in public places, particularly where there is the opportunity for eavesdropping, compromise and theft

5.2.9. Access, view or download any illegal or inappropriate material. The use of internet and email facilities is permitted subject to the same rules as are set out in those policies

5.2.10. Stream content (i.e. play back of audio or video files without being completely downloaded first) unless a wireless connection is used

5.2.11. Let any personal use of Trust mobile devices interfere with your working day – for example make personal calls whilst clocked on
5.2.12. Access any personal email account on your mobile device
5.2.13. Redirect Trust emails to personal email accounts
5.2.14. Let anyone else use the mobile device or transfer your device to another member of staff
5.2.15. Share your passcodes, PIN or password used to access mobile devices allocated to you with anyone else
5.2.16. Leave mobile devices unattended including when travelling, in unlocked offices, unattended vehicles or any other insecure location
5.2.17. Use a mobile device abroad without first informing ICT
5.2.18. Connect any device not managed by the Trust to the corporate network, however you may make use of public wireless capabilities where they are available

6. Other Mobile Devices

There are occasions where mobile devices provided by other organisations and agencies for use by Trust staff may require use of the Trust's corporate wireless network (e.g. iPads provided to medical students by University of Manchester). Where there is such a requirement, IT Department will work with the benevolent organisation to ensure that devices can be utilised within the Trust without compromising the Trust network.

B7 Asset Management

UPDATED AUGUST 2018

1. Who this policy applies to

1.1. All users

2. This policy should be read alongside:

2.1. Access control policy
2.2. Mobile device policy

3. Introduction

3.1. ICT assets must be identified, inventoried and controlled
3.2. There must be robust procedures in place for the procurement, deployment, maintenance and disposal of assets in order to manage the asset life-cycle
3.3. ICT assets include physical hardware such as devices, removable media and communication equipment and software owned by the Trust and procured through the IM&T Division
3.4. A number of asset types are not covered by this policy:
  3.4.1. Medical devices
  3.4.2. Information assets

4. The Trust's commitment

4.1. All ICT assets – hardware and software must be procured via ICT who will ensure best value for money using the relevant procurement frameworks
4.2. ICT will ensure the compatibility and strategic fit of any new assets in line with the Trust's eHealth programme
4.3. The planning and procurement of assets of significant value must be approved by the Trust's IGSG. The Chair of the IGSG will determine the financial value that requires IGSG approval
4.4. ICT will maintain the asset management system
4.5. All new assets will be delivered to IM&T to ensure formal registering of the asset. All received assets will be:
  4.5.1. validated against the original order to ensure correct goods have been supplier
  4.5.2. booked into the IM&T receipting system prior to asset tagging
  4.5.3. securely stored in the appropriate IM&T equipment storage area
4.6. Once the destination of the new asset has been determined, the asset will be prepared for deployment within the Trust
4.7. Prior to deployment, all new assets will be:
  4.7.1. tagged with a unique asset reference where appropriate
  4.7.2. registered on the ICT Asset Management system with a minimum dataset to include supplier, serial number and specification
  4.7.3. assigned an asset owner
4.8. Periodic maintenance of all ICT assets will be carried out either by ICT Support or nominated contractors with the relevant expertise pertaining to the asset
4.9. All ICT assets must be disposed of in line with Trust disposal of asset policies (e.g. capital asset disposals), statutory regulation pertaining to the disposal of the asset (e.g. WEEE regulations, Control of Pollution Act) and Information Governance standards (e.g. removal of data and software etc.)

4.10. For the purposes of disposal, hard drives containing data will be dealt with as a separate asset and an audit trail showing disposal maintained

4.11. IT assets will be disposed of through a specialist contractor subject to the following conditions being met:

4.11.1. the contractor will have a minimum of Level 2 compliance with the Information Governance Toolkit

4.11.2. the contractor will be certified by the Environment Agency under the Control of Pollution Act

4.11.3. data storage media are destroyed in the presence of ICT Support staff

4.11.4. destruction certificates are provided by the contractor for all assets disposed of

4.11.5. logs of all equipment including asset numbers and/or serial numbers are provided by the contractor

4.12. ICT will ensure the asset management system is updated to reflect the disposal of any ICT assets

4.13. Audits will take place to ensure existing assets are still in use and allocated in accordance with the asset register – these will be based on a random sample of assets taken from the asset management system

4.14. Assets which cannot be accounted for will be reported to the Trust's Information Security Officer and a full investigation will be conducted, the results of which will report to the Trust's Information Governance Steering Group

5. Your commitment

5.1. You must:

5.1.1. As an asset owner, ensure that the ICT Service Desk is informed prior to the movement of any ICT asset so that the asset register can be maintained and updated

5.1.2. Advise ICT of faulty or redundant ICT assets

5.1.3. As an asset owner, ensure that all ICT assets are return to ICT for disposal should they become faulty or redundant

5.1.4. Ensure that any assets under your ownership are reasonably protected in terms of security and appropriate use

5.1.5. Advise ICT if an asset transfers owner

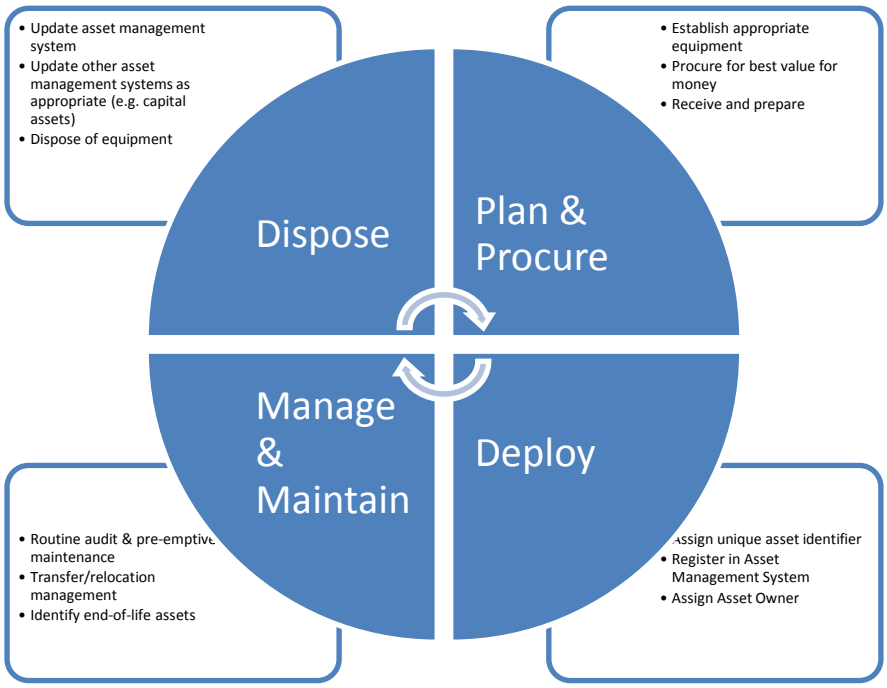
5.1.6. Alert ICT immediately if an asset is lost, stolen or goes missing

5.2. You must not:

5.2.1. Procure any hardware or software without involving ICT

5.2.2. Move any ICT asset that normally has a fixed location (e.g. PCs, printers) without approval from ICT. This not only ensures the accuracy of the asset register but also ensures that relocated assets have the necessary infrastructure to function in any new location

6. ICT asset life-cycle management



B8 Business Continuity and Disaster Recovery

UPDATED AUGUST 2018

1. Who this policy applies to

1.1. All users

2. This policy should be read alongside:

2.1. DR plan

3. Introduction

3.1. The Trust recognises that IM&T systems are increasingly critical to the running of its business and that any loss of key systems could be detrimental.

3.2. The ability to recover the functionality of critical IT systems in the event of a disaster is considered to be essential to the Trust therefore the Trust must ensure that appropriate measures are in place to be able to restore IM&T facilities to be able to maintain Trust business activities in the event of a major failure or disaster.

3.3. This applies to all IM&T systems supported by East Lancashire Hospitals NHS Trust. Systems provided and supported by 3rd parties for example HSCIC (e.g. Choose & Book, HSS Radiology Information System etc.) and Siemens Healthcare (PACS) are outside the scope of this policy and disaster recovery is the responsibility of the relevant 3rd party

3.4. The main computer suites are housed at Royal Blackburn Hospital – there are 2 data centres operating in an active-active arrangement

4. The Trust's commitment

4.1. Systems will be in place to enable the restoration of critical IT systems to support the Trust in the delivery of its services

4.2. Appropriate business continuity plans will be in place with all procedures documented

4.3. Appropriate measures will be in place to safeguard security and confidentiality

4.4. All systems (hardware, software, applications, etc.) will have appropriate support provisions (usually through contracts with third-parties)

4.5. The data network is designed for resilience enabling the reinstatement of service following a disaster on one site and has appropriate maintenance provision

4.6. All data centres, computer rooms, etc. have appropriate facilities for the provision of air conditioning, electrical power and other services, that resilience has been incorporated into the design, appropriate maintenance contracts are in place and regular life-cycle reviews are carried out

4.7. The use of a virtualised server environment, centralised data storage and backup facilities provides the ability to move applications between physical devices in different locations very quickly. This means virtual services can be re-provided quickly and easily

4.8. A daily backup regime is in place to ensure all services are backed up as required. All backups are checked on a daily basis and tests carried out to ensure their integrity. More detail is given in section 6

4.9. The technical specification of all hardware is documented including the details of the applications running, location, details of backup strategy and contract for maintenance

4.10. Alternative arrangements for housing computer equipment are available should existing facilities be made unusable because of failure/disaster,

4.11. A facility to have access to IT technical support is available at all times

4.12. The IM&T disaster recovery plan will define the Trusts recovery strategy – procedures will be in place to counteract interruptions to business activities from the effects of major failures or disasters

4.13. The Trust aims to enable normal working to be resumed in the shortest possible time

4.14. Risk assessments and business impact assessments will be used to identify and priorities the Trust's critical business systems. These will be undertaken with system managers and reviewed by the IGSG as appropriate

4.15. An appropriate level of resilience will be incorporated into the design of every system to mitigate risks due to component/sub-system failure.

4.16. The Disaster Recovery Plan will take into account our business continuity procedures and will include:

4.16.1. The identification of IM&T systems

4.16.2. the identification an prioritisation of critical business processes based on risk assessment

4.16.3. the determination of the potential impacts of various types of disaster

4.16.4. the identification and agreement of all responsibilities and emergency arrangements

4.16.5. the documentation of agreed procedures and processes

4.16.6. appropriate education of staff in the execution of emergency procedures

4.16.7. testing

4.16.8. updating

4.17. The plan will specify clearly the conditions for their activation as well as the individuals responsible for executing each component of them

4.18. Testing of plans will be carried out to ensure effectiveness – a phased approach will be necessary due to the scale of the plan

4.19. The plan will be regularly updated

4.20. The master plan will be kept in electronic format on the Trust's central file storage facilities however several copies will be kept to ensure availability when required

5. Your commitment

5.1. You must:

5.1.1. Store data on networked files servers wherever possible to ensure routine backup are taken

5.1.2. Ensure data stored on devices not always connected to the Trust network (e.g. laptops) is held securely and that encryption is used. (NB. All Trust laptops are encrypted as standard procedure)

5.1.3. Report all incidents relating to data security

5.1.4. As a system manager, ensure that risk assessments in relation to the systems within your service area and the provision of robust business continuity plans are carried out

5.1.5. As a business process owner, be responsible for emergency procedures, manual fall back plans and resumption plans as follows:

5.1.5.1. emergency procedures – the immediate action to be taken following a major incident which jeopardises business operations and/or human life

5.1.5.2. fall back procedures – the action to be taken to move essential business activities to alternative temporary locations

5.1.5.3. resumption procedures – the action to be taken to return to normal full business operations

6. Backup regime

6.1. Current technology in use – Backup Exec 2016

6.2. Hardware – dedicated servers back up to tape library. 2 tape libraries in data centres at Royal Blackburn Hospital replicating between themselves

6.3. Live SAN environment (containing all centralised data storage) backed up to tape once a week with tapes stored off site

6.4. Physical server estate (50 servers) back up separately

6.5. Exchange (mail) backed up to dedicated tape library. No replication in place

6.6. Maintenance window – daily 6pm to 6am

6.7. 30 days backup kept on tape library, all catalogues kept for past 12 months, dailies kept for a week, weeklies kept for a month, monthlies kept for a quarter (3 months) and yearlies kept for ever

6.8. Home drive data is backed up to the cloud

B9 Disaster Recovery Plan

UPDATED AUGUST 2018

1. Who this policy applies to

1.1. All users

2. This policy should be read alongside:

2.1. Business continuity and disaster recovery policy

3. Introduction

3.1. A variety of controls are in operation to ensure high availability of IT systems and services. These include:

- 3.1.1. Resilient infrastructure design incorporating redundancy and minimisation of single points of failure,
- 3.1.2. Environmental controls in all computer rooms including power, air conditioning to manage temperature and humidity, fire detection & suppression, and physical and logical security.
- 3.1.3. Comprehensive multiple-layer backup and archiving procedures
- 3.1.4. Comprehensive data protection including Antivirus, patch management, encryption, end-point security, malware detection, etc

3.2. This plan covers information systems in use within the Trust including all Trust owned endpoints, data network and server equipment. Externally hosted systems are excluded

3.3. A disaster is defined as 'an unplanned incident that results in a significant or total loss of vital computer systems for a period of time that would affect business operations adversely'

3.4. A disaster could arise from damage to, loss or destruction of critical parts of the IM&T infrastructure and the non-availability of information systems (for example resulting from a malware attack)

3.5. Temporary loss of service resulting from equipment malfunction, data cable breaks, application system malfunction, etc., would not normally be classified as a disaster

3.6. Examples of disaster scenarios include:

- 3.6.1. Loss of site/building/computer room/data closet; due to fire, flood, denial of access, wilful or accidental damage
- 3.6.2. Loss of system(s); due to hardware/software failure,
- 3.6.3. Loss (or partial loss) of data network affecting multiple end users
- 3.6.4. Loss of services; power, telecoms

4. The Trust's commitment

4.1. Aims to minimise the duration of a serious disruption to services and minimise the risk of injury, damage and losses

4.2. The Trust will provide interim arrangements to achieve acceptable levels of service

4.3. IM&T will work to reduce the probability of incidents occurring

4.4. The plan will be tested at least every 12 months. Each system should be regularly tested with the outcome documented. This may take the form of operational testing or as part of routine maintenance (for example a system upgrade)

4.5. Plans will be reviewed annually, although more regular updated may be required in response to significant changes to the technical infrastructure including the introduction of new systems and reconfiguration
4.6. If IM&T become aware of an incident which may develop into a major failure/disaster, they will escalate to the Trusts management structure as defined in the Major Incident Plan. This is explained at section 6
4.7. Silver command is responsible for planning and coordinating the response and recovery phase of the incident and will undertake some strategic functions as detailed in the Major Incident Plan
4.8. The Silver Commander will work with Bronze Command to predict likely problem areas and to devise strategies to minimise their impact to Trust business
4.9. Bronze Command will work with end-user departments and IT system managers to bring into operation their business continuity plans
4.10. The IT Recovery Team (ITR Team) will initially comprise the Associate Director of Performance and Delivery, Head ICT, Head of Systems and their immediate managers. Additional members will be co-opted as and when required. The function of the ITR Team is to lead on the technical aspects of recovery and restoration of service and will report to the Bronze Commander
4.11. The ITR team will:
4.11.1. Determine what emergency procedures need to be carried out
4.11.2. Perform a preliminary damage assessment
4.11.3. Estimate possible impact (identify which systems/services affected and to what extent)
4.11.4. Estimate probable repair time and outage period
4.11.5. Liaise with Bronze/Silver Command
4.11.6. Invoke the third party Disaster Recovery contract if required
4.11.7. Liaise with IT System Managers
4.11.8. Initiate and oversee recovery.
4.11.9. Ensure a Recovery Event Log is kept
4.12. The initial aim will be to restore services, even a reduced service, by whatever means possible
4.13. In the longer term, permanent repairs will be carried out. These will be planned and project managed using IM&T procedures and resources

5. Your commitment

5.1. You must:
5.1.1. As a department manager or System manager, ensure that contingency business continuity plans are developed, kept up to date and tested regularly

6. Declaration of major incident procedure

6.1. During working hours:
6.1.1. Service desk inform IM&T manager
6.1.2. IM&T manager informs Associate Director of Performance and Delivery
6.1.3. Trust Director on-call informed
6.1.4. Trust Director on-call declares a disaster and establishes Silver Command
6.2. Outside working hours:
6.2.1. Out of hours service desk informed and escalate immediately to 2nd line support

6.2.2. 2nd line support establishes the facts
6.2.3. If a major impact is suspected, 2nd line support contacts senior on-call IM&T manager
6.2.4. Senior on-call IM&T manager contacts Associate Director of Performance and Delivery
6.2.5. Senior on-call IM&T manager contacts Trust on-call manager who will then contact on-call Director
6.2.6. Trust Director on-call declares a disaster and establishes Silver Command

B10 Access control

ADDITION DECEMBER 2017

1. Who this policy applies to

1.1. All users of Trust information systems

2. This policy should be read alongside:

2.1. Password policy
2.2. Acceptable use policy
2.3. Mobile device policy
2.4. Physical security policy
2.5. Clear screen & desk policy

3. Introduction

3.1. The reliance on electronic information systems continues to increase across the Trust
3.2. Unauthorised access to this information could lead to data loss and misuse
3.3. It is essential that access to these systems is controlled and continually reviewed to minimise the threat of unauthorised access
3.4. Users should only have access to systems that they need and user accounts should be disabled as users leave the organisation
3.5. The principle of 'least privilege' will be used. This means that every program and every user of systems should operate using the least set of privileges necessary to complete the job
3.6. Systems in this context refer to both network access (to the local area network, wide area network and external connections such as the internet) and access to individual information systems

4. The Trust's commitment

4.1. Appropriate processes will be in place to enable users to request access to the required systems
4.2. Appropriate equipment and systems will be provided to enable staff to make best business use of electronic communications systems
4.3. Information systems, application and networks will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information
4.4. All network and information system infrastructure will be located in physically secured and controlled environments and any unauthorised access will be reported as a security incident
4.5. The network will be adequately segmented to protect sensitive systems from unauthorised access
4.6. Information systems will provide user authentication facilities to control access but also to provide audit trail functionality. These will offer a minimum of enforced password entry, or more sophisticated authentication technology e.g. smartcards, security tokens or biometrics.
4.7. Where technically possible, all standard accounts that are delivered with operating systems will be disabled, deleted or have the default passwords changed following installation

4.8. The Trust will work to remove individual application logons by aligning application accounts with network accounts and introducing simplified logon processes
4.9. Unique user accounts will be used across all systems so that users can be linked to and made responsible for their actions
4.10. The use of group identities will only be permitted where they are suitable for the work carried out (for example service accounts)
4.11. A starters, leaver and movers process will be maintained to control those users who have access to the Trust network
4.12. All user workstations will be configured to lock automatically after a period of inactivity in order to reduce the risk of unauthorised access
4.13. Access to the organisations information assets will be limited to those who have the necessary authority and clearance
4.14. Users will be granted access only to the functionality and information required to facilitate their role
4.15. The Trust will regularly review users with access to systems to ensure only the appropriate users have access and that the level of access is commensurate to their role
4.16. Unused accounts will be monitored and appropriate action taken to disable and delete these accounts. This will include the removal of any associated access rights
4.17. The use of network infrastructure and information systems will be monitored to ensure adequate protection from security threats. Evidence of misuse and unauthorised access attempts may be used to provide evidence for security incident investigations
4.18. All forms of remote access will be securely controlled

5. Your commitment

5.1. You must:

5.1.1. Ensure that you follow the appropriate application processes in order to request access to any Trust information system
5.1.2. Provide a form unique identification as part of your application for your network user account – this will be kept securely and will only be used to ensure unique user accounts
5.1.3. Keep any authentication technology items such as security tokens and smartcards safe at all times and report any loss of such items immediately using the appropriate route
5.1.4. Confirm that you are an authorised user as part of the network log on process
5.1.5. Change your passwords when prompted to
5.1.6. Lock your screen whenever you leave your desk to reduce the risk of unauthorised access
5.1.7. As a manager, report any staffing changes through the starters and leavers process
5.1.8. Ensure that you inform ICT or the relevant system administrator if you feel that your account details have been compromised
5.1.9. Ensure that access to information processing applications under your control is strictly managed
5.1.10. Keep all confidential information secure, use it only for the purposes intended and do not disclose to any unauthorised third party

5.1.11. Store confidential or sensitive documents in your personal directory (e.g. My Documents) which is accessible only to yourself. Be aware that documents in shared directories are accessible to others

5.1.12. Ensure that you use the appropriate request form if you require remote access to any Trust system and make sure that you are aware of the additional security requirements in the mobile device policy

5.2. You must not:

5.2.1. User another person's logon details to access any Trust system

5.2.2. Share your application account details with anyone else

5.2.3. Share any authentication technology items such as security tokens and smartcards with anyone else

5.2.4. Attempt to disable, defeat or circumvent any security facility on any computer system

5.2.5. Access the Trust network or any Trust system from a non-Trust owned and managed device

5.2.6. Use any system in a way which may damage, overload or affect the performance of the system or the internal or external network

5.2.7. Download or upload any Trust information to unauthorised removable media devices or remote non-Trust managed locations

5.2.8. Plug in any non-Trust owned network device to the Trust's infrastructure

B11 Clear desk, clear screen

ADDITION DECEMBER 2017

1. Who this policy applies to

1.1. All users of Trust information systems

2. This policy should be read alongside:

2.1. Access control policy
2.2. Password policy
2.3. Physical security policy

3. Introduction

3.1. A quick departure from your computer screen can turn into an hour away from your desk whist your screen may be exposing sensitive data in plain view to all who pass by
3.2. To improve the security and confidentially of information, the Trust has adopted a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities
3.3. This aims to ensure that all sensitive and confidential information, whether it be on paper, a storage device or a hardware device, is properly locked away or disposed of when it is not in use
3.4. This will reduce the risk of unauthorised access and viewing of potentially sensitive or confidential information, loss of and damage to information during and outside of normal business hours or when areas are left unattended

4. The Trust's commitment

4.1. Office areas should be locked when they are not in use
4.2. A secure access system will be maintained to ensure that only authorised personnel have access to staff areas
4.3. Suitable secure areas such as lockable drawers, cabinets, safes and secure rooms will be made available
4.4. Secure shredding facilities will be made available
4.5. All user workstations will be configured to lock automatically after a period of inactivity in order to reduce the risk of unauthorised access
4.6. ICT will carry out ad hoc reviews to ensure compliance with this policy

5. Your commitment

5.1. You must:
5.1.1. Allocate time in your day to clear away your paperwork
5.1.2. Ensure that your desk is clear at the end of the day – with confidential information locked away
5.1.3. Ensure that files containing confidential information are locked securely in desks, filing cabinets or designated secure rooms at all times, other than when being used by staff. All efforts must be made to keep this information secure and not readily accessible to non-authorised staff
5.1.4. Take necessary steps to protect information that is being dealt with during the working day
5.1.5. Remove all information from white boards and any papers following meetings in meeting rooms

5.1.6. Lock away any portable computing devices or mass storage devices, including encrypted USB drives) when not in use
5.1.7. Scan paper items and store them electronically where you can – disposing of the original copy securely
5.1.8. Use designated confidential waste bins or cross line shredders for sensitive or confidential information
5.1.9. Ensure that any confidential printing is collected immediately and not left unattended
5.1.10. Remove any smartcards from card readers when you have finished using it to avoid possible smartcard misuse, loss or theft
5.1.11. Lock your screen whenever you leave your desk to reduce the risk of unauthorised access – you can do this by pressing *CTRL+ALT+DEL* and clicking *Lock this computer* or simply press *Windows Key + L*. (The windows key can usually be found in the bottom left of the keyboard and looks like a flag/window)
5.1.12. To unlock press CTRL+ALT+DEL and log back in
5.1.13. Log off from your machine if you are going to leave it for an extended period of time
5.1.14. Ensure that computer screens are angled away from the view of unauthorised persons
5.1.15. Ensure that computer terminals are shut down at the end of the working day and when there will be no further immediate use
5.1.16. Report and breach or potential breach immediately in line with the incident management policy

5.2. You must not:
5.2.1. Dispose of confidential waste in regular waste facilities
5.2.2. Make use of any straight line shredders
5.2.3. Leave a computer terminal logged on when it is unattended
5.2.4. Attempt to disable, defeat or circumvent any security facility on any computer system
5.2.5. Leave sticky notes containing sensitive information such as passwords, visible on your desk or stuck to your monitor

B12 Patch management

ADDITION DECEMBER 2017

1. Who this policy applies to

1.1. All users of Trust information systems
1.2. System administrators

2. This policy should be read alongside:

2.1. Mobile device policy

3. Introduction

3.1. The Trust acknowledges its responsibility for ensuring the confidentiality, integrity, and availability of electronic data stored on its Information Technology (IT) systems.
3.2. We are obligated to provide appropriate protection against the risk of malicious software (malware) threats, which could adversely affect the security of the IT systems and associated data
3.3. Patching software and firmware across all Trust owned and managed clients, servers, network infrastructure, clinical systems and equipment and mobile devices limits the exposure and effect of malware threats
3.4. The Trust accepts the responsibility to patch and ICT equipment and will endeavour to do so as soon as is practically possible

4. The Trust's commitment

4.1. Patches will be applied across the Trust estate and will include:
  4.1.1. Client devices – desktops and laptops
  4.1.2. Servers
  4.1.3. Network infrastructure
  4.1.4. Mobile devices
  4.1.5. 3rd party applications
  4.1.6. Clinical systems & equipment
4.2. Computers that are not owned and managed by the Trust and the Active Directory Forest Root Domain Controller are excluded from this policy
4.3. As the Trust requires certain versions of Microsoft Internet Explorer to be in place for a number of web based applications, this will be excluded from this policy and will be managed separately
4.4. Microsoft patches will be applied for client machines, servers and relevant mobile devices
  4.4.1. A monthly schedule will be followed and patches will be rolled out through a staged testing and deployment process
  4.4.2. The testing schedule involves deployment through a proof of concept and then pilot groups before staged deployment to the rest of the estate
  4.4.3. The proof of concept and pilot groups must identify and issues relating to applied patches – failure to complete this process will be taken as acceptance and approval to move to the next stage
  4.4.4. Critical patches will be deployed immediately, outside of this process
  4.4.5. Where software has become unsupported, the relevant endpoint will be upgraded to a supported version at the earliest opportunity
  4.4.6. Where endpoints cannot be upgraded due to operational restriction, the endpoint will be secured and hardened to the highest level possible

which may include local firewalling, separate VLANs or being removed from the domain

4.4.7. Where Microsoft release emergency patches for previously unsupported software, these will be applied immediately subject to CAB (change advisory board) approval

4.5. Non Microsoft patches for 3rd party products will be deployed to client machines and servers

4.5.1. These patches will be managed separately as their deployment becomes more complex due to the reliance of line of business applications for certain versions (for example the version of Java required by ESR)

4.5.2. A patch scanning tool will be used to identify any required patches

4.5.3. Patches will be deployed on a quarterly basis in a separate phase to Microsoft patches to ensure that the source of issues can be identified

4.5.4. A staged testing and deployment process will be used

4.5.5. The testing schedule involves deployment through a proof of concept and then pilot groups before staged deployment to the rest of the estate

4.5.6. The proof of concept and pilot groups must identify and issues relating to applied patches – failure to complete this process will be taken as acceptance and approval to move to the next stage

4.5.7. All devices will be updated to the latest version possible – exceptions may be required where devices have a reliance on an older version to support an existing line of business application

4.6. Network infrastructure devices, both hardware and software will be patched to the latest possible version

4.6.1. This includes switches, routers, gateways, bridges, firewalls, SAN (Storage Area Network) and NAS (Network Attached Storage) devices and non-Microsoft servers

4.6.2. Firmware and patch updates will be reviewed every 12 months and the required upgrades will be carried out over the following 4 months

4.6.3. Where devices have become unsupported, they will be upgraded to a supported version at the earliest opportunity

4.6.4. Where devices cannot be upgraded due to operational restriction, it will be secured and hardened to the highest level possible which may include local firewalling, separate VLANs or being removed from the domain

4.6.5. Where emergency patches or firmware upgrades are advised, these will be implemented immediately subject to CAB (change advisory board) approval

4.7. All mobile devices including phones and tablet devices which do not run with a Microsoft operating system will have appropriate patches applied

4.7.1. Such patches are usually released as a reaction to an identified vulnerability or to release new features and end users have to trigger such updates

4.7.2. Patches will be tested on a small number of devices before being pushed to the entire estate

4.7.3. Functionality will be introduced to ensure that users accept these updates such as limitation of device functionality until the update is installed

4.8. Clinical systems and devices will be dealt with on a case by case basis

4.8.1. It is expected that system suppliers will carry out such updates

4.8.2. The Trust may complete update work in the event that suppliers do not support patching of their systems
4.8.3. Where updates are not possible, the system or device will be secured and hardened to the highest level possible which may include local firewalling, separate VLANs or being removed from the domain
4.8.4. Reassurance around compliance will be gained by the Trust
4.9. Devices which are identified a not having patches applied may be blocked from the network
4.10. Once a patch has been deployed, it will be loaded onto the base image for that device
4.11. All patching will be as non-disruptive as possible and users will be given as much notice as possible if a reboot of a client device is required.
4.12. Attempts will be made to carry out any reboots resulting from the patching regime out of hours to minimise disruption caused and users will be made aware of such disruption
4.13. Appropriate testing schedules and backup exercises will be carried out in all cases to ensure that a recovery position is possible if a system needs to be reverted following a bad patch
4.14. The Trust will review the outcome of each patching exercise and the risk level of failed patches considered. Failed update deployments may be investigated and remediated
4.15. The Trust may conduct assessments to ensure compliance with this policy. Any system found in violation of this policy shall require immediate corrective action
4.16. Penetration tests will be used to identify vulnerabilities across all system and the appropriate remedial action taken

5. Your commitment

5.1. You must:
5.1.1. Accept all patches that are published by the Trust and follow instructions to reboot devices when required
5.1.2. Contribute to the patch testing cycle if you are part of the proof of concept or pilot user groups and complete any required sign off
5.1.3. Report any suspected issues relating to patching to ICT immediately
5.1.4. Ensure that clinical systems / devices under your control are full patched by the supplier

5.2. You must not:
5.2.1. Fail to reboot machines when requested
5.2.2. Do anything to circumvent the patching process
5.2.3. Remove any patches from any device
5.2.4. Introduce or use any unpatched software

B13 Printing

ADDITION AUGUST 2018

1. Who this policy applies to

1.1. All users

2. This policy should be read alongside:

2.1. Clear desk, clear screen policy

3. Introduction

3.1. The previous Trust print strategy was unmanaged and uncontrolled with printers being sited on or near desks and personal workstation and no standardisation of settings

3.2. There remains a requirement for printing across the Trust – however the volumes will continue to decrease as the move to digital continues

3.3. Centralising printing will enable a more cost effective and efficient approach to printing, scanning and photocopying across the Trust

3.4. Centralised MFDs will also enable the standardisation of settings to help reduce costs – colour printing costs 10 times more than black and white

3.5. The implementation of secure print will also help to reduce the risk of any ICT security and information governance breaches

4. The Trust's commitment

4.1. The Trust will provide a fleet of managed multi function devices (MFDs) across all sites and all areas

4.2. Training will be provides as the devices are deployed and user guides and other useful information will be available on OLI. This will include how to replenish paper and toner

4.3. The current supplier is Canon – the Trust will manage this contract centrally

4.4. Canon will be responsible for the addition, changing, removing or moving of all devices covered by their contract

4.5. The location of all devices will be centrally managed and controlled by ICT – MFDs will be sited in central locations and printing areas created which will also include secure waste facilities

4.6. All usage of the devices will be audited and monitored

4.7. Software will be used to enable Finance to recharge each department for their usage of MFDs across the Trust

4.8. Colour devices will only be supplied where there is an approved business case

4.9. MFDs will be used for printing, scanning and photocopying

4.10. Although these devices are fax capable, existing fax machines will continue to be used until an appropriate solution resulting from process and requirement analysis is agreed.

4.11. All consumables and maintenance will be included in the contract – this includes an automatic replacement function

4.12. All MFDs will be configured in power save auto shut off mode

4.13. All devices will automatically default to double sided printing

4.14. All devices will be standard black and white default printing. Some devices will be configurable for colour printing

4.15. Each tray in a device will be set up for and loaded with a media type – e.g. plain paper, labels etc. This will be in line with local procedural/operational processes and requirements

4.16. Supply of media including paper will continue to remain the responsibly of the local departments

4.17. Follow you or pull printing will be implemented as standard on all MFDs. This enables flexibility for a print job to be picked up from any device regardless of location, removing the restriction to print to a particular device. Due to application constraints, this feature may not be available on some systems

4.18. Secure access printing will be enabled as the standard default on all MFDs requiring all users to identify themselves at the MFD before releasing any prints or being able to scan or photocopy. This will be facilitated through the use of tap on, tap off technology using existing ID badges. Due to application constraints, this feature may not be available on some systems

4.19. To ensure maintenance of security and to avoid print server overload, the maximum period a print job will be retained and available for printing is 24 hours

4.20. Specialised printers will be implemented where required for example wristband printers. These **MUST** be approved and implemented by ICT

4.21. All individually networked and local printers and scanners will be removed once the new MFD is in place and fully tested – any devices that fall outside of the MFD contract and agreed print strategy will not be supported

5. Your commitment

5.1. You must:

5.1.1. Think before you print – is what you are printing absolutely necessary

5.1.2. Consider using multi-image-per-page printing where possible

5.1.3. Delete your print jobs from the device if they are no longer required

5.1.4. Ensure that you always use an approved Trust MFD for printing, scanning and photocopying

5.1.5. Ensure that you secure all your print jobs

5.1.6. Always present your identification card

5.1.7. Report the loss of your identification card straight away using normal Trust procedures – this avoids the possibility of unauthorised use of the card to access confidential print jobs

5.1.8. Reload paper and remove any jams whilst you are printing your items. If this is left and then resolved by a different user, the rest of your print job will be printed out. This poses a risk of confidential information lying around

5.1.9. Report any issues with MFDs to the ICT Service Desk who will coordinate with the supplier

5.1.10. Make any requests for additional devices to the ICT Service Desk

5.2. You must not:

5.2.1. Introduce any alternative methods of printing, scanning or photocopying by obtaining a relevant device or by negotiating an individual contract with any company without reference to ICT

5.2.2. Order any consumables for standalone devices – these purchases will not be approved

5.2.3. Allow anyone else to use your identification card to release prints
5.2.4. Leave any information on a device – if you see something left from another user, you must drop it into confidential waste
5.2.5. Move any MFD to an alternative location – if this is a requirement, contact the ICT Service Desk
5.2.6. Override the default settings unless absolutely necessary
5.2.7. Print in colour unless you are authorised to do so – colour printing should only be used when and where critically and operationally necessary
5.2.8. Use the MFDs for production of personal materials

B14 Passwords

ADDITION AUGUST 2018

1. Who this policy applies to

1.1. All users

2. This policy should be read alongside:

2.1. Access control policy

3. Introduction

3.1. Passwords are one of the most important things that protect our systems and information. It is important that you use an appropriated secure password and protect it so that it cannot be misused

3.2. In protecting our systems, passwords identify you – so someone with access to your password can impersonate you by transacting or sending emails in your name

3.3. Methods to get hold of your password are becoming more advanced, therefore users should ensure that they keep their passwords safe

3.4. Securely formatted passwords are not easily guessed and are not words found in the dictionary, user account names, the word 'password', proper nouns, birthdays, telephone numbers and license plate numbers

3.5. Passwords are not only used to log onto the Trust's network, but also individual information processing systems – it is essential that this data is kept secure

4. The Trust's commitment

4.1. The Trust will enforce the use of passwords to ensure that access to NHS systems, devices and information is controlled and restricted to approved and authorised users only

4.2. All users will be created an unique password to be used by individuals for each system to which they require access

4.3. Systems will be configured to enforce good password practice where possible

4.4. Network accounts will have complex passwords enabled

4.5. The Trust will implement tap on, tap off technology to assist in the log on process

4.6. The default expiry of passwords will be set to 90 days

4.7. ICT will monitor network passwords and inform user where weak passwords are found

4.8. Systems will be configured to ensure that following the incorrect entering of a password a specified number of times, the account is locked and can only be opened/reset through a system administrator process

4.9. System administrator accounts will require more complex passwords – they will be configured to be minimum 15 characters in length

4.10. Separate login and passwords will be required for administrators to undertake their normal day to day user functions

4.11. No passwords will be incorporated into the hard coding of user accounts in application code

4.12. All new or reset password will be changed immediately upon first log on

4.13. The Trust will provide a self-service user reset functionality for network access accounts

5. Your commitment

5.1. You must:

5.1.1. Use passwords that are hard to guess

5.1.2. Use a password that is longer than 8 characters

5.1.3. Keep passwords confidential at all times

5.1.4. Create secure passwords that can be memorised

5.1.5. Include a mixture of the following:

5.1.5.1. Upper and lower case characters a-z, A-Z

5.1.5.2. Digits 0-9

5.1.5.3. Special characters `!"£$%^&*()-_=+[]{};:@'#~\|<>,.?/

5.1.6. Consider choosing two short unrelated words and concatenating them together with a special character between them, e.g. calf?sheep, cat@snow, film+cup (DO NOT use these specific examples)

5.1.7. Consider choosing a sentence from a song, poem, book, film or phrase and use the first letter of each word. For example, the sentence might be: 'I Will Remember My Password With Ease', and the password could be: 1WrMpW3! – using the first letters of each word and a special character, or may be some other variation. (DO NOT use this specific example)

5.1.8. Consider using nonsense words that are pronounceable and meaningful to you, but not to anyone else, e.g. eeksohno (DO NOT use this specific example)

5.1.9. Change passwords on a regular basis or when prompted to by the system

5.1.10. Protect passwords whilst typing them in, to ensure that they are not disclosed to someone looking over your shoulder

5.1.11. If you suspect unauthorised password disclosure or unauthorised user/application account access, report the incident as a security incident AND, if possible, change your password(s)

5.1.12. If someone asks for your password, refer them to this document or request they contact the ICT Service Desk

5.2. You must not:

5.2.1. Use the same password across multiple systems

5.2.2. Use passwords that you use for accessing personal information processing systems e.g. at home

5.2.3. Disclose passwords to anyone, including system administrators, managers, personal assistants, co-workers, family and friends unless authorised by ICT Services

5.2.4. Disclose passwords over the telephone to anyone, including to persons who claim to be system/ application administrators or ICT

5.2.5. Allow anyone else to use your password or use anyone else's password to access any Trust system

5.2.6. Write down passwords

5.2.7. Store passwords on your PC or email them

5.2.8. Electronically store and transmit passwords without guidance from ICT Services

5.2.9. Reveal passwords in questionnaires or forms

5.2.10. Provide any indication of password formatting used to anyone

5.2.11. Use the ‘Remember Password’ feature of applications and software

5.2.12. Use passwords that are considered insecure:

5.2.12.1. Use your name or the name of a relative, friend, pet or co-worker

5.2.12.2. Use any other personal information such as birthdays, addresses, phone numbers, license plate numbers, the type of car you drive

5.2.12.3. Use your login name in any form (as-is,reversed, capitalised, etc)

5.2.12.4. Use normal words found in the dictionary (english and foreign)

5.2.12.5. Use obvious choices like ‘password’

5.2.12.6. Use proper nouns e.g. town or city names

5.2.12.7. Use names affiliated with the Trust, its services, and locations e.g. Blackburn, Burnley, Hospital, Trust

5.2.12.8. Use all the same digits or characters

5.2.12.9. Use keyboard key sequences, e.g. qwerty

5.2.12.10. Use any of the above preceded or followed by a digit, e.g. secret1, 1secret

5.2.12.11. Use dictionary words where ‘I’s are replaced with ‘1’s, ‘E’s are replaced with ‘3’s, ‘A’s are replaced with ‘4’s, etc

5.2.12.12. Use any of the above spelled backwards

5.2.12.13. Use the same password as a previous one, but with a minor change such as adding the number 1 e.g. hackme1, hackme2

B15 Removable media

ADDITION AUGUST 2018

1. Who this policy applies to

1.1. All users of Trust information systems

2. This policy should be read alongside:

2.1. Access control policy

3. Introduction

3.1. Removable media takes many forms (jump drives, flash memory storage, portable storage devices, etc.)

3.2. Removable media can be personal, removable, and portable which although appears a convenient way of storing and moving information, introduces risk into the organisation whenever it is used to store Trust information

3.3. Apart from the chance for loss and theft, removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations

3.4. Controls are required to ensure that data is available where it is required and that the integrity and security of data is maintained

4. The Trust's commitment

4.1. For the purposes of this policy, removable media shall include:

- 4.1.1. Flash drives and flash memory storage
- 4.1.2. SD storage
- 4.1.3. Removable fixed drives and portable caddies
- 4.1.4. Re writable CDs or DVD media
- 4.1.5. USB remote storage devices

4.2. Removable media storage of any type will be prohibited unless a valid business case for its use is provided

4.3. Those removable media devices whose use is required will be approved by ICT Services

4.4. Technical controls will be introduced to police the black and white listing of such devices

4.5. Encrypted removable devices will be provided where an appropriate business case is in place – these will be managed by ICT Services

4.6. The use of removable media devices will be monitored

5. Your commitment

5.1. You must:

- 5.1.1. Inform ICT Services in the event that a new removable media device is required
- 5.1.2. Only use removable media devices supplied by ICT Services where a business case has been approved
- 5.1.3. Only use approved removable media devices for the purposes of Trust business
- 5.1.4. Ensure that data stored on an approved removable media device is also stored on the Trust's network

5.1.5. Ensure that any authorised removable media is not left unattended when in transit and remains in an authorised employee's physical control at all times
5.1.6. Ensure that removable media is kept in a secure safe or a locked cabinet and returned to safe storage at the end of each work day
5.1.7. Report any actual or suspected breaches in information security immediately – this includes loss or theft of removable devices
5.1.8. Return any removable media devices to ICT Services when no longer required to ensure appropriate disposal

5.2. You must not:
5.2.1. Store any passwords for a removable media device with the device
5.2.2. Use personal storage devices with Trust hardware or for the storage of any Trust information
5.2.3. Use damaged or faulty removable media devices
5.2.4. Connect any approved removable media device to non-Trust computers
5.2.5. Compromise any approved removable media device or the information stored on them in any way
5.2.6. Allow any third party to access data or extract information from the Trust's network without explicit agreement from ICT Services