Leicester City NHS
Primary Care Trust

POLICY DOCUMENT

Information Security Policy Part Two: Detailed Requirements

Approved by:	Commissioning & Governance Committee
On:	February 2011
Review Date:	April 2011
Expiry Date:	April 2012
Directorate responsible for Review	Information& Corporate Performance Directorate
Policy Number:	Corporate 021
Signature:	

Equality Impact Assessment

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race, Ethnic origins (including gypsies and travellers) and Nationality	No	
	• Gender	No	
	• Age	No	
	• Religion, Belief or Culture	No	
	• Disability – mental and physical disabilities	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**Is there a need for external or user consultation?**	No	
4.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
5.	**Is the impact of the policy/guidance likely to be negative?**	No	
6.	***If so can the impact be avoided?***	N/A	
7.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
8.	**Can we reduce the impact by taking different action?**	N/A	

Leicester City PCT Information Security Policy Associated Detailed Requirements.

DOCUMENT CHANGE CONTROL

Date	Version	Author	Reason
October 01	0.1	Vicky Hill	Initial Draft
August 02	0.2	Vicky Hill	Post Audit Review
March 03	0.3	Vicky Hill	Final Draft for Approval
January 08	0.4	Vicky Hill	Update in line with standard 27001. Plus introduction of encryption tools.
May 10	0.7	Vicky Hill	HIS annual review and update in line with local policies

Ref. Change Control: all requests for change to vicky.hill@leics-his.nhs.uk

CONTENTS

1	**PURPOSE**	
2	**BACKGROUND**	
3	**SECURITY ORGANISATION**	
3.1	Risk Assessment	
3.2	Security Responsibilities	
3.3	Legal Compliance	
3.4	Surveillance	
4	**GENERAL AWARENESS**	
4.1	Enabling the Flow of Information	
4.2	Private Work	
4.3	Clear Desk Clear Screen Policy	
4.4	E-messaging (including Email), Intranet, Internet Access and Monitoring	
4.5	Virus Control and Software Regulation	
4.6	~~Offsite (and Home) Working~~ Remote and Mobile and Wireless Working	
4.7	Access Controls	
4.8	Data and Software Exchange	
4.9	General Physical Security	
4.10	Incident Readiness and Management	
5	**MANAGEMENT AND TECHNICAL**	
5.1	Physical Security	
5.2	Electronic Commerce	
5.3	Network Management (including Wireless Network Management).	
5.4	System Operation, Control and Housekeeping	
5.5	System Planning and Acceptance	
5.6	Security in Application Systems (Data Validation**)**	
5.7	Business Continuity Management	
Appendix	**Contacts and Glossary of Terms**	

1 PURPOSE

The purpose of these requirements is to give detailed information relating to the policy statements made in the Information Security Policy Part One.

2 BACKGROUND

During 2001 the NHS IM&T Security Manual (IMG5242) was replaced by British Standard BS7799 as a guide to good information security practice in the NHS and subsequently updated as the British and International security standard (ISO/IEC 27001, 27002:2005, BS 7799-1 , 7799-2:2005

This paper reflects these standards and the guidance provided by Connecting for Health (CFH).

NHS organisations are required to gain a basic level of compliance with the standard through the CFH Information Governance Toolkit (IGT). NHS organisations are not expected to gain formal British Standard certification in the short term.

3 SECURITY ORGANISATION: RISK MANAGEMENT AND COMPLIANCE

3.1 Risk Assessment

LLR will use Risk Management procedures to estimate threat probability, including security risks to information systems and assets; their vulnerability to damage, and impact of any damage caused. Measures will be taken to ensure that, where possible, each system, asset and process is secured to an appropriate and cost effective level, that data protection principles are complied with, and that information assurance and risk is reported to the Board by the SIRO.

Supporting Activity
Overview of the Risk Assessment Process

Assets *Identify major assets of the Trust*
Values *Assess asset value in terms of their importance to the business and/or their potential value*
Threats *Identify appropriate list of threats (Catalogue of Threats)*
Vulnerabilities *Identify an appropriate list of vulnerabilities (Catalogue of Vulnerabilities)*
Risks *Identify measures of risk based on a combination of asset values and assessed levels of related threats and associated vulnerabilities*
Security Requirements: *These are determined by the three main sources namely, those risks identified by the risk assessment process, legal, regulatory and contractual requirements and organisational principles, objectives and requirements.*
Security Controls: *From the above, determine the security controls best suited to protecting the organisation against threats, reducing vulnerabilities and limiting the impact of incidents.*
Reduce Risks: *Assess the degree of reduction due to the above controls selection.*
Risk Acceptance: *Acceptable or unacceptable? For unacceptable risks, decide whether to accept or select further controls.*

Reference the Trust Statement of Applicability and the Control Objectives / risk reductions identified in Part One, Section 2 of this Policy.

The Trust Information Asset Owners and Information Asset Administrators are responsible for monitoring and reporting information risk/ assurance to the Trust SIRO on both HIS supported key systems and on other departmental or local information stores.

The SIRO is responsible for reporting Information Security Assurance to the Board on a regular basis.

Risk Assessments, including Privacy Impact Assessments (PIA) will be conducted with regard to every system, including CFH systems, and will assess compliance with relevant security policies and procedures to ensure good working practices. Assessments will be included in the System Level Security Policy, and subject to regular review. System and service Risk Assessments ,~~take place regularly and~~ are the responsibility of each manager (Information Asset Owner, Information Asset Administrator) with systems responsibility, and of LHIS Senior Management (IAAs).

Risks to information security will be identified, assessed and managed.
Risks may be identified as a result of

- Operational control and implementation of systems and support services in accordance with this policy by the Health Informatics Service
- Operational Control of the key clinical information systems by the Trust.
- Review of new systems including Information Sharing Agreements (ISAs).
- Audit review and spot checks
- HIS system security review
- Capture and review of information security incidents and weaknesses (including user reports)
- Information security advice from DoH and CFH
- Legal or business changes
- Media report
- Trust management and review of key systems
- Risk assessments/ PIAs initiated by new systems or assets, business or legal change, third party access requests, patient access requests.

Risk assessments will be held securely and should include a clear definition of the scope: -

- Identification of assets and threats (the threat may not necessarily be of disaster proportions, such as fire, but may also be 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 (Risk Treatment options)
- Formal report as appropriate.
- Decision to accept or to treat the risk as part of the Trust Information Security Management System.

Where risks cannot be managed at System level, they will be escalated to the HIS/Trust level Risk Register and reported to the Trust IAO.

Significant risks identified by Trust managers (IAOs/IAAs) and HIS managers (IAO/IAAs), will be reported to the SIRO.

3.2 Security Responsibilities

3.2.1 Definition of Security Responsibilities

Specific Information Security Responsibilities for the PCT will be defined as a part of role responsibilities/ job descriptions, policy and policy awareness, and in the LHIS/Trust SLA.

Specific and extensive responsibilities are defined in job descriptions for

The Trust SIRO
The Trust Head of Information Governance
The nominated Trust IAOs and IAAs
The nominated HIS IAOs and IAAs
The LHIS Information Security Manager

All staff are required to adhere to governance and security policy by contract and user responsibilities are outlined in the staff handbook (a part of the staff contract).

Security responsibilities which apply to all staff are further detailed in
- Trust and HIS Mandatory training
- Trust and HIS Induction training, including local departmental induction
- Security and governance awareness information

3.2.2 Security Awareness

Formal recruitment procedures and information security awareness initiatives will include training in information security and the need to protect patient privacy. All staff will be required to complete a confidentiality agreement within the contract of employment. Formal confidentiality agreements will be incorporated into contracts with agencies providing temporary, contract or maintenance staff. Users will be aware of information security responsibility to reduce risk of human error, theft, fraud or misuse of facilities.

- Staff will be required to complete a confidentiality agreement within the contract of employment and informed of the need to adhere to the Information Security Policy and the Data Protection Policy.
- Confidentiality agreements and reference to Information Security and Data Protection will be incorporated into contracts with agencies providing temporary, contract or maintenance staff. Other contract staff will be required to sign an agreement to abide by the same codes of conduct (including confidentiality), and discipline as permanent staff.
- Job descriptions will 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.
- All staff will be appropriately trained and fully aware of their personal responsibilities in respect of information security and that they are competent to carry out their designated duties. Training requirements should be regularly assessed and refreshed.
- 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 the Code of Business Conduct will raise staff awareness of information security and the Data Protection Policy and induction/ starter package will support staff in the course of their work.

- The Information Security Policy and associated Detailed Requirements will be published and otherwise made available to all employees.

3.3 Legal Compliance

LLR will comply with this policy in conjunction with current legal obligations, European Union directives, common law and with the best practice policies and statements of the NHS and of the LLR to maintain information security and confidentiality.

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 LHIS or by contracted staff, on behalf of the PCT only will be the property of the PCT and therefore Crown Copyright.
- The intellectual property rights over software developed by LHIS or by contracted staff, for more than one organisation within LLR (excluding UHL) will be Crown Copyright and the property of Leicester County and Rutland PCT, the host organisation of LHIS on behalf of LLR (excluding UHL), and, should the hosting arrangement change, will be transferred to the 'new' host.

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

Relevant legislation, including existing NHS policies and existing LLR policies must be complied with. (Ref. http://nww.Leicestershire.nhs.uk/ and access 'NHS Information Governance Guidance on legal and professional Obligations', Department of Health).

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

- Each PCT will have 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 staff have a responsibility to prevent unlawful disclosures of personal information.
- The PCT will be separately registered under the Data Protection Act for relevant purposes annually.
- Information will only be used for the purpose for which it was intended.

Ref: 'Data Protection Policy'.

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

Access to systems will be authorised and controlled.

Access to and use of cryptography will be controlled in accordance with legal requirements, CFH guidance and with the policy of the PCT.
Evidence required against a person or organisation within LLR, will be collected in accordance with any published standard or code of practice for the production of admissible evidence. (Ref. PCT Information Governance Readiness for Incident Investigations Policy).

3.4 Surveillance

Surveillance can be undertaken only with the consent of the proper authorities and in accordance with law.

Under the Regulation of Investigatory Powers Act (RIPA), there are two main categories of surveillance; intrusive and directed.

Intrusive surveillance is defined by RIPA as covert surveillance which is carried out in relation to anything taking place in any residential premises or in any vehicle and involves the presence of an individual on those premises or in the vehicle. NHS bodies **CANNOT** undertake intrusive surveillance. The power to do this rests with the Police, Customs & Excise and the Security Services.

Directed surveillance is defined as covert surveillance which is not intrusive, and is undertaken for a specific investigation, and in a manner likely to obtain private information about a person, and is otherwise than by way of immediate response.

- Health bodies (Trusts, Strategic Health Authorities and Primary Care Trusts) can undertake directed surveillance in fraud related cases, with authorisation of the Regional Counter Fraud Operational Team and with the approval of the Chief Executive.
- Chief Executives of public bodies, including health Trusts, PCTs, and Strategic Health Authorities, are NOT empowered to undertake directed surveillance in non-fraud related cases.

Surveillance should not be considered without obtaining advice and guidance from the organisation's Local Counter Fraud Specialist or Local Security Management Specialist.

Any surveillance undertaken must be logged in a Surveillance Log.
.

4. GENERAL AWARENESS

4.1 Enabling the Flow of Information

Person Identifiable (PID) Information

The PCT is fully committed to the Caldicott Principles regarding the protection and use of PID, 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 will be reduced to the minimum essential for the purpose. Where possible all data should be made anonymous;
- Access will be strictly "need to know" and in accordance with the guidance in "How We Use Your Information in the NHS".
- All staff will understand their responsibilities and comply with the law;
- PID information must not be shared with unauthorised persons.

The Trust will ensure that all secondary use data is managed in line with legal obligations.

Sharing data / information with partner organisations

LLR 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:

- Other NHS Trusts and Services (including NHS Provider Trusts, East Midlands Ambulance Service, Mental Health Trusts and other Primary Care Trusts)
- Third Party NHS Trusts
- Agencies working on behalf of Trusts
- Social services;
- Education Services;
- District Councils
- Other Local Authority Services
- Voluntary Sector providers;
- Independent Sector providers;
- Independent GP Practices (Under both PMS and GMS contracts)
- Independent Pharmacists, Opticians and Dentists

An Information Sharing Protocol exists which the Trust signs with partner agencies and specific Information Sharing Agreements will be developed with partners where specific information needs to be exchanged on a regular or routine basis, making the security controls for the protection of information explicit rather than implicit and in line with Caldicott requirements.

Sharing data with non-partner organisations
In addition to partner organisations, the LLR organisations receive regular requests for person-identifiable information. Organisations requesting such information include:

- Police
- Insurance companies
- Solicitors

Whilst such requests may be legitimate, LLR will ensure the use of such information is not abused. For further information Ref: Data Protection Act 1998, Subject Access Request Policy or related policies, Information Sharing Protocol, NHS legal obligations with regard to consent.

Whilst such requests may be legitimate, LLR will ensure the appropriate policies and procedures are in place for staff to follow. Further information is contained in the Data Protection Act 1998, Subject Access Request policy or related policies, Information Sharing Protocol, NHS legal obligations with regard to consent. If in doubt about information sharing with the above organisations staff must seek advice from their line manager in the first instance.

4.2 Private Work

The conditions applying to the use of PCT IT equipment and services for personal purposes will be published and made known to users.

Supporting Activities
The following conditions apply to use of PCT 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. (This does not apply to the provision of private healthcare services).
- When using IT equipment and services for private work, the E-messaging (including email), Intranet, and Internet Access and Monitoring Policy of this organisation must be complied with.
- 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 Remote and Mobile and Wireless Working outlined in the policy.
- No information or software should be loaded which would compromise the use of equipment for work purposes.
- No software should be loaded onto trust equipment without express permission of the LHIS IT Support Manager.
- Where the use of IT equipment and services for personal purposes is permitted, the user obtaining, recording or, storing information must do so in compliance with the Data Protection Act; ensuring appropriate notification to the Information Commissioners Office.

4.3 Clear Desk Clear Screen Policy

Regulations will be implemented to protect premises, information and IM&T equipment from security threats and environmental hazards in order to prevent loss, damage or compromise. (Physical Security).

Supporting Activities
PCT staff will use a clear desk and clear screen policy to reduce the risks of unauthorised access, or accidental damage to or loss of sensitive or confidential information.

The provision of healthcare often involves constant use of confidential information in areas open to the public where it is vulnerable to unauthorised access. In addition, visitors, some temporary and contract staff, security and cleaning staff, are examples of people with authorised access to secure, access controlled sites, who are not authorised to view confidential or sensitive data. The nature of the data and not site location should dictate how and when these requirements are applied. Where confidential (personal identifiable) or other sensitive (e.g. employee's pay scale) information is involved, at the end of each session users will: -

- Remove all sensitive information from the workplace and lock away, in a drawer or preferably in a fire resistant safe or cabinet. This includes all person identifiable information, as well as other sensitive (person or business) information such as salaries and contracts.
- Store visit, appointment or message books in a locked area when not in use.
- Angle computer screens away from the view of patients and visitors.
- Set password protected screen savers to activate when there is no activity for a short pre-determined time period.
- Store paper and removable storage media in secure cabinets or safes.
- Set key lock and password control facilities on PCs, and terminals and lock or log out when leaving them unattended.
- Locate photocopiers, printers and fax machines, so as to avoid unauthorised use and, on printing sensitive documents, remove them from the printer immediately.
- Ensure that post-it notes and sticky labels holding patient-identifiable or other sensitive information are not left to public view.
- Before a patient enters a consulting room, remove all evidence of the previous patient from view (computer screens, medical records, test papers or samples etc).
- Lock all consulting rooms and office areas when they are not in use.

The reception desk can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times, in particular medical records should not be left open and with other personal identifiable information, should not be held on the desk or within reach/sight of visitors or patients.

4.4 E- Messaging (including Email), Intranet, Internet Access and Monitoring.

Policies and procedures will operate which ensure appropriate use of e-mail and the Internet and other electronic messaging in order to protect LLR from embarrassment, criticism or litigation.

Ref. **E- Messaging (including Email), Intranet, Internet, Access and Monitoring Policy.**

4.5 Virus Control and Regulation of Software

Regulation on the use of software will minimise exposure of LLR to unauthorised use of software and to inadvertent import of malicious software. Measures will be implemented to detect and remove computer viruses and malicious software in order to protect information systems, applications and networks.

4.5.1 Virus Control

Protection against malicious software will be implemented by raising user awareness, controlling system access and by change controls.

All users have responsibility for preventing the introduction of computer viruses or other malicious software by adhering to the rules for the regulation of software and complying with virus control procedures.

To minimise exposure to the inadvertent import of malicious software, it is essential to check all computer media entering or leaving the organisation before use; including that being imported or exported by the network. LLR will implement processes to detect and remove computer viruses, including:

- Firewall connections to N3, to screen exchange of data or software.
- Certified virus check software will be installed on all servers (including email servers), in use within this organisation and will be updated regularly. Certified virus check software will be installed on all PCs with automated updates from the servers.
- Users will be briefed on the dangers of malicious software and on virus check procedures.
- Virus cleaning and eradication products will be updated in accordance with schedules laid down by the manufacturer.
- Managers with responsibility will ensure, as far as is practicable, that all computer media leaving this organisation is virus free.
- Managers with responsibility will ensure that all computer media used on their systems and which has come from an external source are checked for viruses.
- Managers with responsibility will ensure that adequate backup procedures are established and documented.
- Managers with responsibility will conduct regular review of systems and will investigate the presence of any unapproved files or unauthorised amendments.
- Wherever possible computer media will be write protected.

Procedures for handling malicious software, including denial of service and hoaxes, will be published. Attacks will be reported through established incident management procedures. (Ref. Incident management).

Business continuity plans will include recovery from virus and denial of service attacks.

LHIS will report incidents to CFH as required and will action any Audit, CFH, or Trust identified security warnings received appropriately.

4.5.2 Software Regulation

All staff will be made aware that the following controls are applicable to LLR systems and that a breach may result in disciplinary action:

- All software installed on equipment (including screensavers, shareware, freeware, and gain ware, and mobile code) must have prior permission from the LHIS IT Support Manager.
- Only licensed software may be used, (Microsoft Office Professional and Windows is licensed for all PCs).
- Software supplied must not be copied.
- Where a software product is needed on additional machines, licences should be extended or additional copies purchased. Requests for procurement of licences should be addressed to the LHIS Service Desk.
- A software inventory is maintained and regular audits of software use may be undertaken.

4.6 Remote and Mobile and Wireless Working

LLR will establish a set of controls and procedures, which will be applied to wireless working, and to all off site working and to remote access activities. This organisation requires users to implement the controls and procedures in relation to secure access and to the transport and use of information, software or equipment off site.

4.6.1 Scope.

This section addresses security standard requirements in relation to wireless, and / or mobile computing and tele-working and emphasises information security and confidentiality requirements for staff who

- Require the flexibility offered to authorised users by wireless connection on site
- Require the flexibility offered by remote access to on site information
- Work from home on an occasional basis (not the main work location).
- Are required to work away from their base location (for example IT support; clinical staff working from a patient's home or at other locations).
- Work in Multi-agency settings whether on NHS or non-NHS bases

When working off site or from home the data protection policies and procedures for the PCT must be followed. In particular data must be secure and any disclosure of person identifiable information must have management approval. When working from home it is preferred that users use an NHS supplied computer due to the support overheads that are otherwise incurred.

4.6.2 Health Staff in Multi-Agency Settings

When working in Multi-Agency settings, health staff should remain mindful that

- In most situations, Health staff do not have authority to share information on individuals without the consent of that individual or the person with parental responsibility for that individual.
- Third party information may not be shared unless with the consent of the third party.
- Consent should be used to support the professional opinion of the health professional in relation to what is necessary to be shared, and never used for carte blanche sharing of information unless specifically required to do so by the patient.
- Patients/ Clients may not be coerced into receiving healthcare including mental health care as this would compromise the care relationship.
- Sharing must be in line with the Caldicott principles.
- Sharing with non-NHS agencies should be supported by an Information Sharing Agreement.

Where pressure to share information highlights security weakness, or increases the likelihood of a breach of confidentiality, this should be reported to line management

and to the Trust Information Governance Lead. Guidance may be sought from the Caldicott Guardian, who is responsible for the confidentiality of patient data.

4.6.3 Authorisation

The use of information processing equipment outside of this organisation, for work purposes, including note books, palmtops, smartcards and laptop computers, projectors and digital cameras, digital recorders, organisers, mobile phones, will be risk assessed, controlled and authorised:

When working offsite or at home the risks increase in relation to

- Loss and theft of equipment and data and including removable media
- Disclosure of confidential information to unauthorised persons
- Access to confidential information by unauthorised persons

Risk assessment should recommend the most secure solutions for the proposed user activity (Contact the LHIS service desk for support).

- Equipment belonging to this organisation will be identifiable to a particular user.
- It is the responsibility of the user to obtain authorisation from their line manager to remove equipment, software or information from their main place of work.
- Only LHIS supplied phones, blackberrys and remote access mechanisms (including Virtual Private Network (VPN)) meet the standards in this Trust security policy.
- The use of user owned equipment with storage devices (including all forms of personal computers, organisers, mobile phones, smart cards), or user owned software, for work purposes, must be risk assessed and formally authorised by line management and subject to confirmed compliance with policy standards for access control and virus checking.
- Use of user owned software and connection of user owned equipment to the Trust network must also be authorised by the LHIS IT Support Manager.
- The connection of any unauthorised devices to the Trust computers or networks is prohibited.
- Personal identifiable or other sensitive work related information must not be held on any personally owned equipment storage device - and also on any personally owned removable media as the Trust has no control over the future ownership of such equipment. If this information is inadvertently stored, the user should seek advice from the Service Desk for its removal (file deletion is not adequate).
- Where equipment is loaned for a period of less than 5 days, only standalone functionality will be provided. Personal identifiable information must not be stored on this equipment. In this circumstance, the password will be held by IT Support and shared with the user. The password/ smartcard/ passcode must not be written down or otherwise held with the equipment**.**

- The Trust adopts a self-insuring approach to its IT equipment. Where equipment used off site (or at home) is damaged or lost, the costs of rectification/replacement will be discussed with the individual user and associated budget holder.
- Limited personal use of NHS provided portable equipment and software is permitted but must conform to the rules regarding private work described in this policy.
- Use of digital voice or imaging recording equipment, including mobile phones, must also comply with the relevant PCT Policy.
- Use of PDAs and mobiles for electronic messaging must also comply with the Trust Email and Internet Access and Monitoring Policy.

4.6.4 Access Control

Whether using networked or standalone equipment, it is the responsibility of the user to apply appropriate secure access controls.

- When on site and wishing to connect to the network using a wireless connection: -
    - Access to the LLR Wireless network and attachment of equipment requires registration of the device MAC address by the authorised user of LLR systems and of the device.
    - Do not install or operate Wireless Access Points.
    - Do not allow wireless equipment to act as a server of any kind.
    - Do not invent or transfer network settings or host identities.
    - Check with the Service Desk for approval and hardware compatibility before purchasing wireless adaptors for end user devices.
    - Please note that when connected to the Trust network on-site, using a cable (i.e. not by wireless access), it is recommended that staff should switch off the laptop wireless switch.
    - Inform your line manager and the LHIS Service Desk when wireless access is no longer required
- Authorised access to organisation systems via network connections will be permitted using accepted security access controls only. When working off-site or at home, it is preferable to use a secure VPN (remote access) connection to access email and shared drive files. This is more secure than carrying information on mobile devices or removable media and enables a user to work as if sitting in the office. Access to application systems by this method is strictly controlled. Staff are strongly advised to use a hardware firewall when accessing via VPN from home.
- Access control functions such as user-id and passwords, smartcards/ passcodes, will be enabled on all equipment; whether linked to the network or used as standalone. Encrypted information is only protected against theft and loss of a laptop or removable media if the rules for password and smart card management and the rules for passphrases are applied. Users should change their password/ passcode whenever they feel it may have been compromised and as prompted by the system.

- PIN numbers must be set on mobiles and PDAs. LHIS supplied Blackberrys must be password protected and with the user name, location and phone number displayed on the front screen).
- When storing information on a laptop, standard operating system password protection can be limited and additional security may be required. In particular, access to data must be restricted to you and denied to others; use directory or file level protection particularly if others have access to your equipment or, contact the LHIS Service Desk for advice.
- Personal identifiable or other sensitive data held on laptops must be encrypted either by use of a hardware encrypted laptop or by applying software encryption to the data.
- Personal identifiable or other sensitive information copied to removable media (tapes, disks, CDs, usb memory sticks), or sent by email must be encrypted. The rules for use of removable media, described in the Data Exchange section of this policy must be applied.
- Personal identifiable or other sensitive information must not be stored on PDA equipment (such as electronic organisers), or mobile phones as these are particularly vulnerable to data loss, equipment loss and to theft.

Note. LLR will, where possible, use browser technology to develop systems for use in the field. These systems will be designed to minimise the amount of data stored on portable equipment so that security will be focussed on sending and receiving/displaying information. Such systems will have built in encryption facilities.

Note. Where existing field systems download unencrypted data to laptops or removable media, steps will be taken to reduce these risks.

4.6.5 Physical Security.

4.6.5.1. Transport of IM&T Peripheral Equipment, Software and Information

Where possible, patient related data must be made anonymous and all personal identifiable files should be encrypted.

Employees will be aware that the security of equipment, software and information carried and used off site is their own responsibility and that they are liable to disciplinary action if they fail in these responsibilities.

- When travelling, users must not leave equipment, software, or information (including manual records, removable media) unattended at any site including, on public transport or, in a car (unless locked in the boot).
- Manual records should be carefully stored; cases should be fastened, preferably locked.
- Where possible, when travelling on foot or by public transport equipment should be hidden or disguised.
- It is inappropriate to work on patient related data or other sensitive information when travelling (for example by train/plane).

- Access to equipment, software or data (including manual records/ removable media) should be by authorised personnel only.
- Guard against breaches of confidentiality when using a mobile telephone.
- Protect equipment and information appropriately from exposure to the elements or to strong electromagnetic fields.

Any breach of security must be reported immediately to the LHIS Service Desk and to the line manager (e.g. equipment or information loss or theft).

4.6.5.2 Use of IM&T Peripheral Equipment, Software and Data Off-site and at Home

'Off-site' working covers a wide variety of environments (including home). Every effort should be made to operate in the most secure way possible. This is particularly true with the handling of sensitive data whether electronic or paper based. The same discipline over the use and disclosure of this information must be exercised as if the work were being done in a controlled office/clinic environment

- When working at home every effort should be made to keep work life and domestic life separate. Designate a particular space in the home. Permit access to this space but ensure the documents and equipment found there are left alone.
- Before any information, particularly paper-based, is taken off-site to work on, ensure that the information will not be required on-site or out of office hours.
- Working off-site is intrinsically less secure than a controlled office or clinical environment. Information may be lost or stolen; and members of the public, or at home, members of the family and visitors, also present a threat to information security. Access controls (previously described) and the following physical controls should be applied
    - Log off from or lock equipment when leaving it, even if only for a few minutes. Authorised password protected screensavers must be used.
    - Store manual records securely; cases, or the home office, or filing cabinets should be locked at all times when not in use (even for short periods). Keys should be held securely. Staff must still adhere to the Trust's procedure regarding the storage of clinical information (ref. Records Management Strategy).
    - Portable equipment or removable media should be placed in a secure cabinet when not being used, and passwords/ pin numbers held separately, and the cabinet key held securely. If dedicated storage is not available, as a minimum, when at home, store equipment and media out of sight, preferably upstairs.
    - Guard against breaches of confidentiality when using the telephone.
    - When working at home, position equipment away from prying eyes, ground floor windows, and sources of heat or dampness (e.g. radiators or water pipes). Ensure that all is secure before leaving the house.
    - When working off-site; whether for support or healthcare purposes (e.g. in a patient's home) ensure that data is not displayed to unauthorised persons.

- When working off site in clinics, schools, offices, or houses (excluding one's own home), equipment, software or data (including manual records), should not be left unattended.

4.6.6 Backup

It is the responsibility of the user to backup data on a regular basis to prevent the loss of critical information. At home or off-site where there is no network link, this should be done to removable disk or CD/ or memory stick using encryption tools. It is recommended that data be loaded to a networked server or system when on Trust premises.

Care should be taken to ensure that data stored on PDA equipment (such as electronic organisers), which can be lost at a touch of the reset button, is backed up regularly.

If the portable system is used for processing patient clinical records then the user must ensure that any changes made are immediately uploaded to the practice/ hospital/ Trust clinical system to ensure that a precise and complete record is maintained.

4.6.7 Virus Control and Software Protection

HIS will ensure that appropriate anti-virus software has been installed on Trust servers and is maintained up to date. Users are responsible for logging into the network regularly to ensure that their portable equipment anti virus protection is maintained.

4.6.8 Maintenance

All waste documentation, printouts and removable media should be returned to the work place and the usual disposal procedures followed.

4.6.9 Accounting and Audit

Software and information held on portable equipment is subject to the same audit procedures as equipment and systems used on-site. This also covers information and data stored on removable media or on staff owned equipment.

4.7 Access Control

Access to all systems, applications and networks will be controlled by authentication procedures commensurate with the sensitivity of the data held within or transmitted across them. Access rights will be authorised by individual managers with responsibility, and access to personal identifiable clinical information will be on a 'need to know' basis. Access to data for secondary use purposes will be controlled in line with the legal obligations of the Trust.

Authorising Access to Computer Systems

4.7.1 Access to Legacy Systems - Procedures and Rules

All staff and contractors are reminded that unauthorised access to systems is a criminal offence.

All staff and contractors are reminded that when accessing data for secondary use purposes the data must be de-identified where appropriate; either anonymised or pseudonymised, in line with the legal obligations of the Trust. Contact your line manager if you are in any doubt as to whether the purpose would permit access to de-identified data only. This applies whether accessing data stored on local drives, local databases, Trust application systems or the Trust Data Warehouse.

Standard levels of access to systems (networks, operating systems, application systems and data warehouses) required by staff groups (and including LHIS staff), contractors or third parties, will be defined. These will reflect business and security needs and relevant legislation (for e.g. Data Protection) and NHS directives (for example, de-identification). User profiles or other access rights will be documented and reviewed bi-annually by line managers and by managers with responsibility for security (IAAs/ IAOs).

The ownership of data in the Data Warehouse will be the determining factor in deciding which organisation has the authority to approve access to the data. Where the owner(s) choose to delegate this authority, this arrangement will be communicated as a written agreement to the HIS to ensure that access requests are requested and approved in accordance with agreed process.

Access requests to information and systems will be determined by line management on a strictly need to know basis and users will be given a copy of the access request made.

Staff will receive application system training prior to using the system in their job role.

Access requests will be accepted only with appropriate written authorisation by line management and an authorised signatory. Requests will be accepted by email from

the account of an authorised signatory. Where access is subject to time restrictions, access outside these hours will be authorised. Where access requested is outside established profiles, authorisation from the Manager with responsibility for system security is also required. Users will receive a copy of the authorised access request.

Human Resources will provide evidence of new starters, change of role and terminations or access to systems will be reported to line management and to Managers with responsibility and the LHIS for review regularly. This and other reporting mechanisms will ensure that unused accounts are investigated and disabled where appropriate.

Except in emergencies staff must not have access to live data over and above that originally assigned; where emergency access rights are granted (to technical staff or engineers), they must be authorised by the Manager with responsibility, granted under a specially allocated user-id, and be password controlled.

Subject to a risk assessment by a senior manager, access rights may be suspended, where an employee is subject to a disciplinary hearing or suspension, with a view to safeguarding the confidentiality and security of the Trust systems and data.

Access rights will be suspended or revoked where an employee or contractor's contract has been terminated. Access rights should be revoked immediately where employment is terminated due to gross misconduct.

Use of system utilities will be restricted, access controlled and monitored.

Where possible and appropriate, terminals will be set to time out.

Users will receive clear instruction that accounts will not be shared.

Where temporary accounts are required these will be authorised and controlled by line management with the agreement of the Manager with responsibility for security.

The use of user- owned equipment with storage devices (including all forms of personal computers, organisers, mobile phones, smart cards), or user owned software, for work purposes, must be risk assessed and formally authorised and subject to confirmed compliance with policy standards for access control and virus checking.

The connection of any unauthorised devices to the Trust computers or networks is prohibited.

Personal identifiable or other sensitive work related information must not be held on any personally owned equipment storage device - (including all forms of personal computers, organisers, mobile phones, smartcards) and also on any personally

owned removable media as the Trust has no control over the future ownership of such equipment. If this information is inadvertently stored, the user should seek advice from the Service Desk for its removal (file deletion is not adequate).

4.7.2 Access to NHS Connecting for Health Systems – Procedures and Rules

Trust policies will follow the national standards and processes identified by NHSCFH with documented, risk assessed and approved local enhancements.

All staff and contractors are reminded that when accessing data for secondary use purposes the data must be de-identified where appropriate; either anonymised or pseudonymised, in line with the legal obligations of the Trust. Contact your line manager if you are in any doubt as to whether the purpose would permit access to de-identified data only. This applies whether accessing data stored on local drives, local databases, Trust application systems or the Trust Data Warehouse.

CFH systems ~~take a different approach to access – in technically permitting access to national systems and data,~~ place some reliance upon staff contract, line managers and 'privacy officers' to monitor staff activity and 'alerts' which is 'after the event' security: -

- Detailed written procedures for each CFH system will document the management controls required to assure local managers, as far as is possible, of the activities undertaken by their staff.
- These to include 'assurances required'. Organisations should seek written assurances that appropriate, agreed controls are in place in other departments, NHS organisations, external organisations with access to health data.

The Trust Registration Authority (RA) Manager will nominate a number of RA agents to verify user access.

The PCT has commissioned the Health Informatics Service to provide RA agents to all PCT and General Practice staff.

RA Sponsors will be nominated to authorise user access.

The RA Sponsor and the RA Agent are responsible for the card issuing process in line with Trust RA policy. The RA sponsor and RA agent will understand the role based access available and how roles are applicable to staff, contractors or third parties.

Use of 'fallback cards,' will be logged and monitored by local management.

Training and support will be made available to sponsors and agents.

Staff will receive application system training prior to using the system in their job role.

Requests for staff access can be made in advance of their start date but must include the expected start date.

All users will be issued with a smart card, user-id: -

- The line manager will report an identified need to the relevant sponsor.
- The user will input a personal passcode/PIN known only to themselves on receipt of the card.
- The sponsor and user will complete form RA02 defining the user roles and business functions required.
- The user and RA Agent (and sometimes the sponsor) review the RA01 in a face to face meeting.
- The sponsor confirms user-id or the user presents photographic evidence and evidence of address.
- The RA Agent will verify the role requirement defined by the sponsor and may challenge the roles assigned.
- The RA agent inputs user details to the Spine.
- The RA Agent issues the smart card to the user and files the RA01 form.

Staff, contractors and third parties will receive instruction never to use another individual's account.

Smart cards and pass codes should always be carried separately.

Staff will sign a statement to confirm the access rights given and their responsibilities.

4.7.3 Leavers

When a member of staff (permanent, contract, temporary, locum) leaves this organisation, line management will ensure that:

- Users have removed any personal data stored on organisation's equipment before it is returned.
- Information from computer accounts or manual records is handed over.
- HIS are informed and all computer accounts relating to the individual are closed
- For NHS CFH systems, the line manager/RA Sponsor will complete an RA form (RA03 of the user is leaving the NHS altogether or an RA02 (to remove all roles) form if the user is remaining with the NHS but not with the same Trust). The form will be used to notify the RA Agent so that all computer accounts relating to the individual may be deactivated.
- The individual is reminded of the terms of the confidentiality agreement and informed in writing that s/he continues to be bound by it
- All IT property is returned as appropriate to the Trust or to LHIS (including swipe cards for physical access to secure areas; strong authentication/ VPN tokens for remote access; laptops; palm tops, usb memory sticks and smartcards if the user is leaving the NHS)

- The individual is asked if personally owned equipment has been used for work purposes and an assessment made as to whether this equipment needs to be reviewed.
- All identity badges, car parking permits and any keys belonging to the organisation are returned

4.7.4 Change of Post

When a member of staff (permanent, contract, temporary, locum) changes post within this organisation, line management will ensure that:

- Access rights to all computer accounts held by the individual are reviewed and LHIS is informed of required authorised amendments.
- For NHS CFH systems, access rights to all computer accounts held by the individual, are reviewed by the RA Sponsor and Agent.
- For NHS CFH systems, changes are recorded on RA02 and the Agent amends the spine record accordingly.
- IT property is returned to LHIS or the Trust as appropriate.
- Identity badges, car parking permits and any keys belonging to the organisation are returned, replaced/ changed as appropriate.
- When moving to another NHS organisation, the individual is asked if personally owned equipment has been used for work purposes and an assessment made as to whether this equipment needs to be reviewed

Note. Where an employee moves to another NHS organisation, their email account will be closed and a new account opened.

Note. When a new member of staff requires use of a PC or telephone line, and none is available, contact the IT Service desk and ensure that orders are placed. It normally takes 6 to 8 weeks to obtain a new PC or to install telephone lines, and with the additional two weeks notice required to set up user accounts, the lead time for ensuring that employees are set up on their start date could be 10 weeks. Equipment needed should be considered at the point at which the post is advertised.

4.7.5 Log-on and Password Standards

Access to all systems, applications and networks will require, as a minimum, the use of a unique user-id and password or a smartcard, pin number and passcode for identification and authentication of users, and for tracking user activity where appropriate.

Password management is the responsibility of the individual employee and must comply with the following standards: -

- Your user-id and password or smartcard, pin number or passcode must never be shared.
- Your user-id and password, or smartcard, pin number or passcode, must never be written down or otherwise recorded, or left close to a terminal or PC or carried with a laptop.

- Temporary passwords, issued by LHIS with the users personal log-on id, must be changed at the first log-on.
- Passwords and passcodes should be a minimum of six alphanumeric characters; a mixture of lower and upper case where possible, and including digits.
- PIN numbers must be 4-8 digits in length.
- Users should change their password or pin or passcode regularly
- Users should change their password or pin or passcode whenever they feel that it has been compromised.
- In the event of a password/ pin/ passcode being forgotten users will be required to identify himself or herself to the password manager (a security question and answer may be required to enable the service desk to identify the call.).
- If you access multiple protected systems, it is acceptable to use a single good quality password, as described above, for all services where the password is stored securely (never displayed) within the system, service or platform.
- Do not use the same password for business and for personal use.

In addition, users will log out at the end of a particular session, or set a screen lock, or set an authorised password protected screen saver where appropriate.

Computer screens should not be left logged in and unattended.

4.7.6 Support/Administrator Access

All privileged (root/ administrator) access to systems which enables override of the usual system or application controls, will be limited to those with a legitimate reason for such access and will be under the strict control of the Manager with responsibility for security and with due regard given to the segregation of duties.

Privileged access may be time limited and monitored by LHIS or by the Manager with responsibility.

Privilege allocations will be checked at regular intervals to ensure that unauthorised privileges have not been obtained.

Temporary passwords will be issued for the purposes of routine maintenance and will be deleted as soon as the work is completed.

Access and use of utilities at operating system level will have secure log-on procedures which may include

- Password control (no display of the password characters, no sending of passwords in clear text over a network
- No display of system identifiers until the logon procedure is complete
- Display a general warning regarding access by authorised users only
- No provision of help messages that would aid an unauthorised user during the logon process.

- No indication of which part of the logon process is incorrect in case of error.
- Limitation of the number of unsuccessful log on attempts
- Limitation of the time allowed for the logon procedure

4.7.7 Remote Access Controls

4.7.7.1 Remote Access by Staff (Remote and Mobile and Wireless Working)

When wireless access is required for working on a local NHS site, access must be approved and the MAC address of the wireless device registered. User requirements are detailed in section 4.6 of this policy.

There is a facility for members of staff to connect securely into the computer network from the Internet, allowing use of e-mail, internet, and access to files off-site as standard. This access is only permitted with the use of a VPN smartcard authentication device.(Ref. VPN policy).

- Remote access can be requested by staff using the appropriate Trust remote access form, authorisation and budget code
- An RA01 form must be completed to obtain a smartcard for VPN use.
- Staff will abide by the Terms and conditions of the VPN specific policy
- Remote access beyond the standard access described above, including to Trust application systems, will not be permitted unless the LHIS receives an instruction from the Trust confirming that such access is in accordance with Trust policy.
- Staff will be required to have their own broadband connection.
- Staff are strongly advised to use a hardware firewall.
- It is preferred that staff use Trust owned equipment for VPN use.
- VPN security will not be reduced if the staff member uses wireless connections at home.

On receipt of an authorised request for remote access, LHIS will

- Grant VPN access to the network for the staff member
- Issue the member of Staff with a secure device (e.g. token, VPN smart card)
- Provide familiarisation training
- In the case of a laptop - configure the PC
- Give advice regarding security and ensure that the member of staff is aware of the VPN policy.

The secure VPN smartcard should be afforded a high degree of protection. The device provides the owner with unlimited access to N3 and ultimately, any clinical system connected to the network if access rights and privileges are provided or breached. Security and confidentiality of patient information could be compromised if a device is lost or stolen.

- Devices/ smartcards must be kept secure and never shared.
- If a device/ smartcard is lost or stolen it is to be reported immediately to the LHIS Service Desk.

If remote access is no longer required, or the member of staff is leaving this employ, the appropriate remote access cancellation form will be completed, in addition, an RA02 or RA03 form will be completed and remote access removed from the users NHS smartcard, or otherwise, in accordance with the rules for smartcard management. It is the responsibility of the staff member and line manager to follow the advice given in this policy for staff members who leave or have a change of post.

4.7.7.2 Staff Access to External Networks

Access by staff to external networks will be governed by formal data sharing protocols including controls to ensure secure access.

4.7.7.3 Remote Access by External Agencies.

Remote access by external agencies will be authorised, securely controlled and monitored.

- Any proposals to allow access by external agencies must be agreed by the LHIS Senior Managers and by the Director with responsibility for IM&T.
- Each supplier or other external user (external honorary, consultant, locum, GP etc.) requiring remote access will be required to commit to maintaining confidentiality of data and information and using qualified representatives.
- All routine maintenance and troubleshooting will be treated as a single authorised session with each access being specifically authorised, enabled and supervised by the appropriate manager with responsibility or a representative.
- Access to computer systems and network will be protected through the use of a firewall for communications with other non-LLR organisations and suppliers across N3.
- Connections not going through the firewall must comply with the N3 Statement of Compliance and procedures for secure remote access (for example, VPN). Where modem links are connected, in response to authenticated supplier request, enhanced modem security incorporating strong authentication measures should be introduced as soon as is practicable.
- No other connections will be permitted.

Responsibilities for reviewing and disabling access rights of external agencies should be agreed with the line manager and with the manager with responsibility for security on confirmation of access levels.

4.7.8 Monitoring System Access and Use

Access to, and use of the Trust's IM&T Resources may be routinely monitored in order to ensure that they are being used only for authorised purposes.

Supporting Activities

Audit logs may be switched on to record exceptions and other security relevant events where practicable and where they will be reviewed. Logs will be held securely. Review will aim to identify

- Access failures;

- Abnormal log-on patterns;
- Use of privileged accounts, e.g. root/ admin access;
- Use of sensitive resources, e.g. access to clinical information.

Logs may be checked monthly for both specified activity and randomly to track individual transactions. Monitoring activity will be agreed with individual managers with responsibility / data custodians and will depend upon the criticality of the system and information; vulnerability from public networks; previous experience; specified need.

Reports will be treated as confidential, and access to monitoring tools will be controlled by senior IT and Audit management.

System or network alerts may result in review of access and use.

In CFH systems, the monitoring of alerts by a privacy officer is required and these will be escalated where inappropriate activity is suspected.

Access to logs will be controlled. Systems and firewall logs may be searched against set criteria and copied to secondary logs to facilitate monitoring.

Monitoring undertaken will be regularly reviewed for compliance with legislation. Audit spot checks may result in review of access and use.

4.8 Data and Software Exchange

The PCT will ensure that control is exercised over the exchange of information including patient-identifiable or other sensitive (personal or business) data, within and between LLR organisations, and with organisations or individuals external to the PCT, to minimise the risk of loss or misuse of data. This concerns risks associated with the use of electronic office systems and both electronic and non-electronic transmissions of data, and verbal communications.

4.8.1 Data and software exchange agreements

For critical or sensitive data formal agreements, (including software escrow agreements or information sharing agreements where appropriate) for exchange of data and software (whether electronic or manual) between organisations will be established. These agreements will specify security conditions and may include:

- Management responsibility for controlling transmission, despatch and receipt.
- Minimum technical standards for packaging and transmission.
- Courier identification standards.
- Responsibilities and liabilities in the event of loss of data and other security incidents.
- Data and software ownership and responsibility for data protection, software copyrights compliance and similar considerations.
- Technical standards for recording and reading data and software.
- Audit of security standards in third party organisations.

Reference the relevant policies of the PCT relating to Data Protection.

4.8.2 Electronic data transmission controls

It is the responsibility of the individual to obtain approval of the Trust Data Protection Officer and Caldicott Guardian confirming procedure for regular and ad hoc exchange of patient-identifiable or other sensitive data to individuals or organisations external to this organisation.

Exchange must be in accordance with the security controls specified in existing Information Sharing Agreements or otherwise authorised by the Director with responsibility for IM&T.

File protection procedures (including encryption and password protection) will be implemented as appropriate.

File control procedures (including confirmation of files sent and received; separation of processed and non-processed files; reliable storage and recall mechanisms) will be implemented.

Standards will be followed for the use of N3 and Internet and E-mail and network security measures (for example, firewalls and routers, modem control, and where appropriate encryption) implemented.

Internal mail may be used to send electronic media (e.g. tape, disk) to NHS organisations in Leicestershire so long as the data is encrypted. New, unused media should be used to send data by tape or disk.

4.8.3 Encryption and transmission of data.

Any intention to send unencrypted sensitive personal identifiable or other sensitive information by electronic means must be approved by the Trust Board and NHS East Midlands and should be reported in the first instance to the Trust IG Lead and the Caldicott Guardian.

Personal identifiable or other sensitive information, in transmission or stored on any removable media or removable device, must be encrypted in order to protect the confidentiality of the data in case of loss, theft or other unauthorised disclosure.

There will be secure management of all keys relating to cryptographic controls, digital signatures etc, whether applied by individual users or by certification.

Where encrypted removable media is to be shared, care must be taken to ensure that the intended recipient has the correct technical capability to de-crypt the data on receipt and this should be established in advance of any sharing of media;

Encryption software installed on all machines can be used to encrypt any digital file including –

- Data downloaded to disk, CD, memory stick or any other removable media.
- Information sent as attachments by email (the Trust's E-Messaging (including email), Intranet, Internet, Access and Monitoring Policy and the leaflet Exchanging Sensitive Information clarify when to use full encryption and when the Trust's own 'encryption in transmission' solution can be employed).

Encryption protects data to a level of 256 bit encryption and is in line with CFH standards.

A passphrase of 20 characters will be required for transmissions of encrypted information not covered by certificate or by the Trust's local secure network solution. The passphrase selected should be

- Alphanumeric and including lower and upper case (minimum of one each)
- Minimum of 20 characters in length
- Maximum 250 characters in length
- Minimum of 2 digits which may not be in the first or last position
- Minimum of 5 symbols (including spaces comma ! " £ $ %)
- Maximum of 2 adjacent character repeats
- Memorable to the sender but not guessable by others
- Not a famous quotation, proverb or saying
- The passphrase will not be written down and left near a PC or with encrypted data.
- Care will be taken to ensure that the data can be re-created/ encrypted in case the passphrase is forgotten.
- The same passphrase will not be sent to the same recipient repeatedly, or random numerical / symbols will be applied to each transmission
- Passphrases will be changed regularly and whenever they have been compromised.

Staff will ensure that the passphrase required for the recipient to read the files is sent by an alternative medium to that used to send the information. For example:

Media	Files to be sent by	Passphrase sent by mechanism
Email	electronic	By phone, post or fax
Disk/CD	By hand to the intended recipient	By hand, By phone, by email,
	By hand to the recipient's site	By phone, by email, by fax
	By internal mail/ courier	By phone, email, fax
	By external mail/ courier	BY phone, email, fax
Memory stick	By hand (memory sticks are not robust enough to be sent by post) and are most useful as a storage medium.	By phone, by email, by fax
Tape	By internal mail	By phone, email, fax
	By external mail	By phone, email , fax
	By hand to the user	Verbal
	By hand to the site	By phone, email, fax.

Amendment of encryption software by unauthorised users is prohibited.

Safe haven protocols for transfer of information by fax will be implemented and users will receive advice regarding communications by telephone, use of mail, voice mail, video communications, internal and external mail and facilities, including courier identification standards. (Ref: Data Protection Policy and the Transferring of Patient Identifiable Information Policy.).

4.9 General Physical Security

4.9.1 Electronic Information Media Security

Where information media (i.e. any removable media including tapes, computer disk, CD, DVDs, usb memory stick) has been used to record patient-identifiable or other sensitive data.

- Personal identifiable or other sensitive information held on removable media for whatever purpose will be encrypted.
- All essential magnetic media will be re-filed in a safe secure environment after use.
- Work files or 'scratch' tapes must also be protected if they contain patient-identifiable or other sensitive information.
- A data storage system that avoids descriptive labels will be used so that unauthorised persons cannot identify data from the label.
- If no-longer required, the contents of any re-usable media that are to be removed from the organisation should be made unrecoverable.
- In order to prevent loss of information when the media lifetime expires, information stored on media that needs to be available for longer than the lifetime of the media must also be stored elsewhere.
- Only where necessary and practical, authorisation by senior management should be required for media removed from the organisation and a record of removals kept in order to maintain an audit trail.
- Where information is to be stored on removable media and sent off-site, new or previously unused media must be used to prevent the inadvertent sharing of additional information.
- The Trust permits the use of hardware encrypted memory sticks only.

4.9.2 Disposal of Equipment and Media (Physical Security)

All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. ~~All removable media holding personal identifiable or other sensitive information and no-longer required, will be securely disposed of~~ Disposal of removable media including CDs, DVDs is managed by the Trust secure, environmentally aware disposal arrangements.

Disposal of assets (e.g. PCs, Laptops) will be controlled by the LHIS IT Support Manager to prevent possible unauthorised access to data. (ref. LHIS Disposal Procedure).

- All PCs, laptops and tapes for disposal must be notified to the LHIS Service Desk.
- All hard disks will be reformatted/ de-gaussed or physically destroyed before disposal.
- If the data on hard disks cannot be overwritten, de-gaussed or repartitioned and reformatted then they will be locked in a secure place until this can be carried out
- Where equipment has a change of purpose or owner all patient-identifiable or other sensitive data will be removed by specialist software (deleting files is not adequate).

- If no longer required, the contents or removable media should be wiped and rendered unrecoverable; if removable media has been rendered unusable then it will be disposed of securely and in an environmentally friendly manner. Guidance will be issued to users regarding disposal of CDs, disks and usb memory sticks (- Ref. disposal procedure).
- Paper medical records will be preserved as per the guidance in the Records Management Strategy.
- All sensitive or confidential paper waste will be securely disposed of in accordance with local site procedures.

Ref. LHIS Procedure for the Secure Disposal of Computer Equipment
Ref. Records Management: NHS code of practice: Parts 1 and 2
Ref. PCT Information Lifecycle Management Policy

4.9.3 System Output

System output classification will be considered in accordance with national guidance. Where systems produce reports, statistics and/or other information a log will be maintained by the manager with responsibility and include a brief description of the information content, frequency of production and the recipient of the information.

Printing: Care must be taken when printing sensitive information. Users will be required to consider where the printer is sited; who has access to the printer; the nature of the data being printed and will be advised to retrieve documents immediately on printing and store safely.

System outputs not required will be destroyed in accordance with rules for disposal of equipment and confidential waste.

4.9.4 Purchase of Equipment by Employees/Leavers

Purchase of equipment by employees or leavers will not be permitted due to Health and Safety considerations and to the administrative overhead that this incurs.

4.10 Incident Readiness and Management

The Trust will be prepared for incident investigation, and will identify information security weaknesses, minimise damage from information security incidents and malfunctions, and monitor and learn from such incidents. Information security incidents will be detected, reported, investigated, and appropriate action taken.

Supporting Activities
In order to be prepared for incident investigation the 'Information Governance; Readiness for Incident Investigations Policy' has been approved by the Trust. This policy is used in the training of Incident Investigation Leads and with the Trust Incident Management Policy, is linked to the capture of information security incidents by the LHIS. Agreed incidents are fast tracked to the Trust Incident Lead and the Trust Head of Information Governance.

Information security incidents are defined as any event that has resulted, or could result, in:

- Disclosure of information to any unauthorised individual
- The integrity of a computer system or data being put at risk
- Non-availability of systems
- Any adverse impact on any individual or organisation, such as loss of privacy, legal penalty, financial loss, embarrassing publicity, disruption of activities or business processes.

LLR organisations and some partner and third party organisations, are responsible for the capture of information systems security incidents and identification of security weaknesses, and for reporting them to LHIS (excepting UHL), to enable appropriate escalation and a timely, effective and orderly response.

- Staff, including LHIS staff will be held individually responsible for reporting immediately any breach, or potential breach of security, which comes to their attention to the LHIS Service Desk.
- Alternative reporting lines will be made available for the benefit of staff reporting suspected security breaches by their superiors and will ensure absolute protection and confidentiality for the party reporting.

Procedures to ensure effective reporting, classification, recording and resolution of hardware software or data security incidents will be established, and ensuring robust links to existing SUI procedures. The impact and costs of unusual incidents will be assessed and lessons learned documented and addressed. Associated information risks will be identified and reported to the IG Lead by the LHIS Information Security Manager, LHIS IT Support Manager, by Trust Management or by Internal Audit.

Details of the incident reporting scheme will be provided to all new members of staff,

at induction and will be available on the Intranet.

Operational applications, systems and networks will be monitored for security breaches where there is reasonable suspicion of abuse.

Copies of logs and incident reporting forms will be held securely and retained for use by audit staff.

Incidents will be reported as required to other bodies and in accordance with legal requirements.

Where appropriate, Internal Audit support will be called upon and particularly where an incident is deemed to represent a disciplinary or possible criminal offence.

A formal disciplinary process will be instigated where employees have violated organisational security policies and procedures.

Ref. LHIS Incident Reporting and Investigation Procedures
Ref. PCT Incident Management Procedures
Ref. 'Information Governance; Readiness for Incident Investigations Policy'

5. MANAGEMENT AND TECHNICAL

5.1 Physical Security.

Regulations will be implemented to protect premises, information and IM&T equipment from security threats and environmental hazards in order to prevent loss, damage or compromise.

5.1.1 Asset Management

The PCT has an appointed SIRO, responsible for information and information systems and their use within the Trust and has designated Information Asset Owners and Information Asset Administrators (managers with responsibility for ensuring risk management and security of information systems, information assets and services). IAAs and IAOs report risks to the JISC and where appropriate, they are incorporated into the Trust risk register and the SIRO informed of key risks by the Head of Information Governance. The SIRO reports to the Board with regard to information risk and assurance.

Each set of logical or physical assets will be allocated a named manager, responsible for information security aspects of all assets within his/her area of responsibility. These managers are the designated IAOs and IAAs.

Information Assets include

- Information assets: databases and data files, system documentation, user manuals, training material, operational and support procedures, continuity plans, fallback arrangements, archived information;
- Software: application and system software, development tools and utilities;
- Physical assets: computer equipment (processors, monitors, laptops, modems, printers), communications equipment (routers, PABXs, fax machines, answering machines), magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
- Services: computing and communications services, general utilities (e.g. heating, lighting, power, air-conditioning).
- People. Their qualifications, skills and experience in use of information systems.
- Others less tangible. For example, the reputation and image of the Trust.

The responsible manager (IAO/IAA) will

- Identify all assets within area of responsibility
- Ensure that information and assets associated with information processing facilities are appropriately classified in line with any national guidance on the classification and labelling of information.
- Confirm and review and authorise who can use the assets and with what type of access and for what purpose.
- Approve appropriate security protection for assets.
- Monitor maintenance, support contract and service level agreements.

- Ensure compliance with security controls including change controls
- Ensure purchase of additional software licences where appropriate
- Ensuring compliance where necessary with the Data Protection Act (1998) and any other relevant legislation to help prevent unlawful disclosures of information.
- Key non-HIS departmental systems, will have a designated IAO/IAA(s).
- Key shared systems will have a designated ~~both an LHIS (technical support) person and a 'Key User' person with responsibility for security~~ IAO/IAA (s).
- All ~~key~~ assets will be clearly identified and an inventory drawn up and maintained including all information necessary for the recovery of key assets from a disaster. ~~(Including a systems and server list, server location, and for each server; a software list, maintenance history, backup activity, recovery plan, owner.).~~
- Assurance regarding secure disposal of assets will be required by the IAA/IAO.
- Acceptable use of assets, including personally owned equipment, will be communicated to users and individual responsibility for secure use made clear. (Ref. Remote and mobile and Wireless Working Policy, and E-Messaging (including email), Intranet, Internet, Access and Monitoring Policy).

5.1.2 Controlled Stationery and Medical Records

Management of secure stationery, such as order forms, prescription pads is in accordance with the Duthie Report. Cheques and other secure stationery in Finance are covered by Standing Financial Instructions. Formal procedures to control and account for the use of such controlled stationery will be maintained within the relevant department and is the responsibility of line management.

Ref. Records Management: NHS code of practice: Parts 1 and 2

Ref. PCT Information Lifecycle Management Policy

5.1.3 Physical Access

IT facilities supporting critical or sensitive business activities where ever practicable will be sited in secure areas, and protected from unauthorised access, damage and interference, by a defined security perimeter, with appropriate entry controls and security barriers.

Supporting Activities

In sensitive computer areas

- Areas will be protected by locks, with codes that can be changed periodically, or by electronic access systems.
- Access to all rooms containing critical IT equipment, such as servers and communications equipment will be restricted.
- Third party support service personnel will be granted authorised, restricted access only when required and this access will be monitored.
- Where possible, Information processing facilities managed by the organisation will be physically separated from those managed by third parties. It is the responsibility of local site managers to ensure that access to all rooms containing

critical IT equipment such as servers, communications equipment, by external third parties is logged and their activity monitored.

In all non-public areas
- Visitors must be supervised, required to wear a visible authorisation badge, and their date and time of entry and departure recorded.
- All staff must be required to wear visible identification.
- Staff with visitors will, if appropriate, ensure that they are accompanied throughout the visit.
- Staff will be instructed to challenge strangers.

Access controls on third parties for example cleaning, catering, security guards, consultants or support staff will be reflected in a third party contract, and including non-disclosure agreements.

All areas of the organisation's premises not requiring public access out-of-hours will be secured, as a minimum by lock and key by 6.00 p.m., or in accordance with documented physical security arrangements for the site, unless by prior authorised arrangement.

Use of CCTV monitoring, photographic, video, audio or other recording equipment will be in accordance with the Data Protection Policy

Physical access controls at each site and secure area will be reviewed regularly. Special consideration will be given towards physical access security in buildings where multiple organisations are housed.

Access to Medical Records will be in accordance with the Records Management Strategy.

Delivery and loading areas will be access controlled or located away from secure areas, and incoming materials will be checked for security hazards.

5.1.4 Equipment Security: Environmental Threats, Theft and Loss

Installation
IM&T equipment must be installed and sited in accordance with the manufacturer's specification and appropriate measures taken to maintain physical security. This should ensure that the terms of warranty are not broken.

IM&T equipment must be sited in locations suitable for maintenance and support functions to be performed, that is, with due regard to the need for LHIS or external support personnel access for prolonged periods.

Eating and drinking is not permitted in designated secure areas housing computer equipment.

All server and associated communications equipment will be housed in secure accommodation protected by, as a minimum, a combination lock and with secure uninterruptible power supplies. Server and communications equipment will be kept physically separate wherever possible. Where possible, rooms housing such equipment will be air-conditioned and where this is not possible, the extremes of temperature and humidity will be monitored.

All rooms containing central server equipment will be protected from fire by a fire monitoring system and will be assessed for danger of flooding. Fire fighting equipment will be provided and suitably placed. Hazardous or combustible materials will be stored at a safe distance from a secure area. Bulk orders of stationery will not be stored in secure areas.

Photocopiers, fax machines will be sited appropriately within the secure area to avoid demands for access compromising information.

All telecommunications cabling will be, wherever possible, physically protected.

Backup and fallback equipment and media will be stored and protected separately, in fire safes or in a separate fire zone where appropriate, or off-site.

Suitable intruder detection systems will be installed in line with PCT policy.

Equipment Maintenance and Support

Critical systems and equipment will be covered by comprehensive maintenance and support (third party maintenance agreements) or by LHIS support staff for its operational life. PCs, terminals, large printers, servers and communications equipment are covered by warranty and will have third party maintenance agreements where it is cost effective. Maintenance agreements with third parties will be specified in formal contracts and will ensure the confidentiality of any data held on that equipment.

Guarantees will be obtained from system suppliers to ensure that critical systems will not be lost for a period longer than 48 hours unless specifically negotiated and agreed. Only approved systems engineers will be allowed access to hardware or software and where possible they will be supervised whilst on site and activity monitored. Remote diagnostic services will only be implemented where it is essential for the effective running of the system.

Individual system security policies will record whether and which disks may be removed from official premises for maintenance or repair. If disks are to be removed the data will be overwritten or the equipment de-gaussed; if this is not possible, the company removing the disk for repair must have in force a security policy regarding de-gaussing/ destroyed equipment and sign a confidentiality clause of non-disclosure which covers all company staff.

All equipment that requires maintenance or repair will have patient-identifiable or other sensitive information removed from it. It is not sufficient to delete files using the operating system. Data will be removed correctly using a third party software application that guarantees approved deletion of files.

If the hard disk has failed and the maintenance engineer is required to replace it with a new device then the old hard disk will be physically destroyed. If the hardware is returned to the supplier for repair a note of all serial numbers will be taken including the hard disk. If the hard disk is irreparable the owner of the equipment will insist that the old hard disk be returned for destruction.

5.1.5 Power Supplies and supporting utilities

Where possible this organisation will ensure there is back-up power to the mains electricity supply at key sites. All key computer equipment must be protected from power failure by uninterruptible power supply (UPS), allowing controlled shut down. UPS equipment should be tested annually. Where appropriate, use of a backup generator will be considered.
Critical computer equipment must be fitted with emergency power off switches for use in a crisis and have circuitry not subject to power surges from other organisations.

Lightning protection will be applied to all buildings.

Adequate supplies of fuel will ensure that generators can perform for a prolonged period.

Water supplies will be adequate to supply air conditioning, humidification equipment and fire suppression systems (where necessary and used).

Telecommunications equipment will have two power supplies fitted to the equipment. Voice services should be adequate to meet local legal requirements for emergency communications.

5.1.6 Cabling

Power and telecommunications cabling carrying data or supporting IM&T services will be protected from unauthorized interception or damage by ensuring that

- Cabling (electricity or communications) between buildings will be via underground conduit not accessible to unauthorised people.
- Cabling between buildings will be fibre optic.
- Cabling within buildings will be in conduits if surface mounted otherwise, within the framework of the building.

Power cables will be segregated from communications cables to prevent interference.

Technical sweeps and physical inspections should take place for unauthorised devices attached to cables.

5.2 Electronic Commerce

LLR will develop e-commerce applications (involving use of EDI, electronic mail and on-line transactions across public networks such as the Internet) with appropriate controls to satisfy the network threats associated with such activity.

Supporting Activity

LLR will use browser technology where possible to develop systems for use in the field. These systems will be designed to minimise the amount of data stored on portable equipment so that security will be focussed on sending and receiving/ displaying information.

E-commerce will be supported by documented agreements between involved parties, which will include specification of liabilities for any fraudulent transactions, authorisation details and security controls

Such systems will have built in encryption facilities, complying with national standards for encryption, to satisfy the need for authentication and vetting and meeting requirements for confidentiality and integrity of transactions.

System design will ensure against incomplete transmission, unauthorised access modification or disclosure or message duplication of online transactions.

Publicly available information will be protected to prevent unauthorised modification.

Faults will be identified from operator logs and fault logging and audit logs will be maintain to aid investigations.

5.3 Network Management (Including Wireless Network Management).

All wide and local area networks will be managed to accepted security standards. These will, as a minimum, meet the requirements set out in the N3 Statement of Compliance and the British and International standard for security.

5.3.1 Supporting activities

The Wide Area Network referred to below is managed by LHIS and serves all LLR organisations excluding UHL. Countywide connectivity is achieved via links to UHL , which have firewall protection, and by LHIS managed connections. Third party controls apply to all non-LLR organisations. A range of controls will be applied to achieve and maintain security in the computer network both for data and for the protection of connected services from unauthorised access.

LLR organisations served by LHIS have signed the N3 Statement of Compliance.

5.3.2 Strategy and Documentation

The strategy for the Infrastructure Architecture will be developed in line with national strategy and the IT Strategies of LLR Organisations; new projects; and with operational exigencies. The Strategy will be reviewed bi-annually and will include an explanation of Network procurement issues and development strategy, and N3 requirements.

A Network description, significant links and resilience issues are documented as part of risk analysis and business continuity plans for the organisation and these are subject to annual review.

An up to date map of the network topology is maintained and includes network infrastructure devices such as servers, routers, switches and firewalls.

Network maps and other documentation is held securely and controlled.

5.3.3 Responsibility and Controls

The Network Manager has operational responsibility for the network, which includes responsibility for security and resilience.

The Network Manager will establish responsibilities and procedures for the management of remote equipment.

The Trust is responsible for informing the LHIS Service Delivery Manager of significant changes in its user requirements (e.g. change of staff location), to enable network planning.

All network management controls and procedures will conform to the N3 Statement of Compliance, to the British and International security standard and to this policy.

WAN controls will be implemented to ensure network availability and to safeguard the integrity and confidentiality of data passing over public networks and to protect connected systems and to prevent unauthorised access to networked services.

5.3.4 Access Control - Preventing unauthorised access to networked services.
No direct connection will be permitted between this wide area network and networks external to N3 except where appropriate controls are implemented. All external connections must be authorised by HIS.

Dial up connections or VPN, including third party access, will be permitted with Strong Authentication controls, and utilising as a minimum, tokens or smartcard VPN access with locked down rules. A remote access server will handle these connections.
Before allowing third party access a risk assessment will establish risks and counter measures to reduce them.

Arrangements for third party access must be based on a formal contract containing, or referring to, all the necessary security conditions to ensure that the organisation concerned can satisfy NHS information security requirements. Contracts may include agreement for this organisation to audit the security arrangements the third party has in place.

Before outsourcing the operation of any systems:
- Ultimate responsibility for information processed by an out sourcing party remains with the Trust.
- Agreement of the owners of the applications concerned will be obtained
- Boundaries and responsibilities of involved parties will be defined clearly
- Implications for business continuity plans will be considered
- The third party must conform to NHS IGT security requirements
- Procedures and responsibilities for managing security incidents will be agreed
- Access controls will be implemented for LLR Organisations staff and contractors (Ref. access control)
- IT facilities management contracts will specify the level of security the supplier should provide, which will be in accord with the system security policy.
- Audit and evaluation of third party security standards will take place.

5.3.5 Information Flow
When planning new connections, due consideration will be given to information security requirements (firewalls, cryptography etc).
- All WAN connections to N3 will be protected by a specialist firewall; which offers greater security. A firewall can only be as secure as the network services that are allowed through it. Only services with a considered business need will be allowed and current government advice regarding services to be blocked will be reviewed.

- Checks will be made to ensure that routers are not running vulnerable or unnecessary network services.

5.3.6 Network Availability
Controls to maintain the availability of the network services and computers connected may include
- Automated Network Monitoring
- Development of in house maintenance expertise
- Support and maintenance agreements
- Built-in resilience with alternative routes and backup equipment (spares)
- Backup of configuration settings
- Disaster recovery and emergency planning
- Regular assessment of external interfaces to the network and the services offered to them and active monitoring and testing of external threats.
- Assessment and monitoring of internal threats.
- All computers, servers, workstations and routers on the network will have logging of security relevant events enabled in circumstances where those logs can be reviewed, so that an audit trail of incidents will be available.
- Logs will be reviewed and automated exception reporting may be implemented.
- Intrusion detection system will be considered in the deployment of replacement or new server equipment.

5.3.7 Authentication
The WAN is a ring-fenced/ walled network with fixed Internet links via N3 Secure Gateway.

VPN links will be used.

EIGRP will be used to provide the most suitable route for network traffic with rapid replication across sites, limiting the need for manual intervention.

Third party fixed links will be secured as a minimum, by the controls offered by N3 Statement of Compliance, Strong Authentication or De-militarised Zone.

Ingress filtering will be applied by firewall controls.

Intrusion Detection System (IDS) may be employed for added internal security.

No modems will be utilised without the express authorisation of LHIS.

5.3.8 Security of Wireless Links
Wireless links including microwave, radio and laser technology, will be considered to enhance the resilience of the network. Wireless communications will utilise cryptography as a minimum level of security. LLR will adopt national guidance/ information security best practice for all such implementations.

Wireless connectivity has been introduced in LLR sites in order to provide flexibility to the user. The Wireless Network Management Policy is a risk assessed system level policy and is held by the LHIS Infrastructure Manager. User facing tenets of this policy are reflected in section 4.6 above (Remote and Mobile and Wireless Working).

5.3.9 Cryptography
Where appropriate and in accordance with national guidance, encryption, digital signatures et al, will be applied.

Legal advice will be sought to ensure compliance with national laws and regulations before encrypted information or cryptographic controls are moved to another country.

5.3.10 Audit
Internal Audit will be invited to review network security, including firewall configuration bi-annually.

5.4 System Operation, Control and Housekeeping

Responsibilities and instructions for the management and operation of all computers and networks will be established, documented and made available to all those who need them.

Supporting activities
Daily and periodic operational control procedures will be documented and implemented to ensure efficient operation and effective control of systems; including day to day operation and backup, system housekeeping; database monitoring and utilisation monitoring leading to optimisation procedures; and operational change control.

Computer operations security measures will be in line with the recommendations given in the standard.

The sensitivity of an application system will be identified and documented by the manager with responsibility. The sensitivity may indicate that the application system should

- Run in a dedicated (isolated) environment
- Share resources within limitations
- Have no limitations

Configuration Management
An effective configuration management system for all information systems, applications and networks will be established.

Networked PCs will be recorded on LAN desk Inventory software and a best practice secure configuration will be used where possible.

Server and network device configurations will be backed up to tape and in secure storage.

Applications will be configured in accordance with supplier instructions

Security software (e.g. firewalls) will be configured according to the manufacturers instructions, audit recommendations and CFH Statement of Compliance.

Housekeeping and Documentation
Procedures will be documented and maintained by the Manager with responsibility. An approved system documentation pack may include:

- User Service Level Agreement
- Data sharing protocols if appropriate
- Risk analysis, including PIA (Privacy Impact Assessment), counter measures and business continuity plans

- Evidence of system capacity to meet growth requirements over 3 years
- System description with inputs and outputs
- Daily and periodical operations procedures (Housekeeping)
- Handling of data files
- Handling of errors
- Disposal of personal or confidential data
- Archive and retention requirements
- Start up and close down procedures
- Equipment maintenance
- Computer room management
- Database management and optimisation procedures
- Backup and recovery and restore procedures
- Safety: protection from unauthorised access, damage, loss.
- Access controls and access security requirements including segregation of duties.
- List of key personnel (manager with responsibility for security IAOs/IAAs, support contacts, user contacts, suppliers, maintenance)
- User manual
- Local user procedures where available.

Systems will have up to date documentation, which reflects the present state of the system with much of the above information summarised in a system level security policy, with annual review and made available to IAOs/IAAs.

Distribution of systems information must be authorised by the relevant manager with responsibility, IAOs/IAAs.

Separate copies of system documentation will be held at different sites where appropriate. The security of systems documentation is the responsibility of the Manager with responsibility, IAOs/IAAs.

All sensitive information including systems, business, patient, and staff information will be kept under secure conditions.

Off site maintenance will be subject to authorisation by a nominated officer and dependent upon an assessment of the status of data held on the equipment.

Fault logs and Operator Logs
Faults shall be identified and corrective action taken. A log of operator activities is maintained on servers and reviewed.

Clock Synchronisation
All PCs are synchronised back to the servers to ensure the accuracy of audit logs and so aid in investigations.

Security of System Files and Programs

Dedicated Applications support / operations staff will be responsible for

- Updating program libraries; previous versions of executable code will be retained
- Maintenance of an audit log showing all changes made
- Software upgrades and application of patches
- Monitoring supplier activity on the system
- Ensuring where possible, operational systems will hold only executable code
- Ensuring access to source code is limited
- Separation of programs under test/ development from operational source code
- Ensuring that program listings are held in a secure environment
- Archiving of previous versions of source code
- Maintenance and copying of program source libraries subject to strict change control procedures
- Responding to requests for test data from operational systems
- Person identifiable information will be avoided or anonymised (by users)
- Appropriate access controls to test data will be implemented
- User authorisation will be obtained before operational information is copied to a test application.
- Applying changes in operating system and including review and testing of applications to ensure that there is no adverse impact on functionality, security, or business continuity (and in conjunction with user acceptance testing).
- Where system changes/ patches are provided by the supplier into the live environment, assurance will be sought regarding the testing of changes on comparable sites/ and where the changes are already live.
- Changes to software packages will be made only with the consent of the vendor and ensuring that maintenance and support agreements are not affected.
- Simple patches to operating system software/ email servers, will be applied in a timely fashion and the version/ version applied date recorded.
- Communication of changes to all relevant persons.

Data Back-up

Procedures will be implemented to ensure that as a minimum: -

- Back-ups are taken daily of all data and essential software on corporate systems and network servers.
- The Trust identifies users responsible for changing and storage of server backup tapes where required.
- Recall and recovery processes are established and tested annually
- Data back-ups are given safe storage away from system location.
- Data is archived appropriately.
- Users are aware of their responsibility to backup ‘C’ or ‘D’ drive data regularly.

Procedures will be implemented to ensure important records are protected from loss, destruction or falsification.

LLR will comply with records management requirements referenced below when minimum system archive requirements are determined. The recommended minimum retention periods apply to both paper and computerised records. Extra care needs to be taken to prevent the corruption or deterioration of computerised records and the re-recording and migration of data will also need to be considered as equipment and software become obsolete.

Ref. Records Management: NHS code of practice: Parts 1 and 2
Ref. PCT Information Lifecycle Management Policy

Utilisation
Utilisation of key IM&T applications and systems will be monitored to ensure the availability of data and systems. Including: -

- HIS Management review of the use of the network, application software and application systems.
- Presentation of a quarterly report on system utilisation and use of the LHIS
- Service Desk facility to the Trust.
- Report and assessment of capacity management requirements.

5.5 System Planning and Acceptance

Systems procurement, software development and changes to new and existing systems, will be undertaken in a controlled manner in order to ensure successful implementation of secure systems. Issues of confidentiality, availability and data integrity will be addressed to prevent the loss, modification and misuse of information and to minimise the risk of systems failure.

Supporting Activities
In order to maintain and protect the integrity of data and of the technological infrastructure, no software development or procurement of hardware, software, or systems will be permitted without the involvement and approval of the LHIS service provider.

Where NHS Framework agreements cover procurements of hardware, and software and including network assets, such procurements will be authorised and documented.

Major procurements and developments will be project based and will comply with POISE, STEPS and PRINCE 2 procedures paying due regard to the systems life cycle. Project management and methodologies will be adapted according to the needs of individual projects and deliverables will be determined by the project board and at PID stage.

The majority of large projects will require the following deliverables PID, analysis of requirements (OBS), ITT, contract, system and acceptance test plans, PIA, implementation plans, risk register, change control log, post implementation review.

Responsibilities within each stage of the project, including commitment of staff time for requirement definition, acceptance testing and cascade training, will be clearly defined for all interested parties and with agreed sign off points.

Project managers will ensure that all parties external and internal, interested in or affected by an implementation are involved in the process or are made aware of its implications. This will include the nominated IAOs/IAAs, and the Caldicott Guardian and Information Governance Lead who should be requested to approve proposed exchanges of patient-identifiable or other sensitive data through the Information Sharing Agreement Approval Process.

Project Managers will ensure that where new processes, systems, or changes are identified, the potential impact on information is assessed using the Checklist for New and Changed Systems, Processes and Services to confirm that the confidentiality, integrity, accessibility and quality of information can be deemed as adequate, maintained and /or improved.

Changes will be formally documented as agreed by all parties.

Projects, where they fall within LHIS remit, will be owned by the user community but supported by HIS. A record of meetings will be kept and all contacts with suppliers of systems will be made through HIS.

Where major procurements and developments benefit more than one organisation there may be issues regarding ownership of hardware, software and data. These issues should be resolved at the PID stage of the project, documented and with facility for review. All new systems will comply with the requirements of the Data Protection Act regarding access to data on a need to know basis and with due regard to organisational boundaries.

All projects will identify security requirements at the requirements phase and these will be agreed and documented as part of the overall business case for an information system, and tested prior to system implementation. The framework for analysing security requirements and identifying controls to fulfil them is risk assessment and risk management.

All contracts with external suppliers of major application systems will be subject to scrutiny by the project board and by solicitors prior to selection (including licensing arrangements, code ownership, intellectual property rights, escrow). System acceptance will follow a formal sign off procedure involving examination of test results and will be completed by the User owner and relevant LHIS Senior Management and quality, accuracy and security checks. The project board will monitor supplier compliance with contract.

System Acceptance will include testing of all links to external systems; functionality and manual procedures (including reference data maintenance, report production); file control and processing, start up and closedown, backup and restart processes, and other routine operational procedures; Access Controls and any other specific security requirements; Communications links and remote input; Performance/ response time/ scalability tests, concurrent input, contingency and business continuity arrangements. All test data when taken from live systems, should be anonymised by users in accordance with the Data Protection Act and Caldicott principles. There will be formal documented handover procedures from system test to user acceptance testing and from user acceptance testing to live operations.

An approved system documentation pack will include security controls.

New operational software will be quality assured.

Information systems, applications and networks, and all connections to external networks and systems will have documented system security controls approved by LHIS Senior Managers.

Change requests to operational systems will be adequately assessed, reviewed d tested (including security implications), and communicated. Acceptance and sign off

responsibilities will be identified for suppliers, users and HIS; change control procedures (including update of all associated documentation) will be followed.

Security of system files and programs will be assured.

The Health Informatics Service may require checks on, or an audit of, actual implementations based on approved security controls. A post implementation review will take place on all projects.

5.6 Security in Application Systems (Data Validation)

The PCT will continue to maintain confidence in data accuracy, completeness and currency for use in decision making, by implementing appropriate controls.

Supporting Activities
Steps will be taken by line management and IAAa/IAOs to select and document appropriate controls in the use of application systems. Working procedures may include clear delegation of authority/ allocation of responsibilities; input validation; processing and output plausibility checks: -

5.6.1 General Controls

Measures will be implemented to reduce the risk of human error, fraud, or theft. In conjunction with previously outlined access controls and retention, disposal and incident procedures: -

- Responsibility for enforcing proper authorisation over data will be clearly assigned.
- Information handling and input is the direct responsibility of the person handling/ inputting the data supported by their line manager.
- Line management is responsible for ensuring that procedures are formally documented and reviewed annually for both manual and electronic information.
- Expertise will be shared and documentation will ensure that critical work could be continued in the event of non-availability of key staff.
- Users will be required to handle confidential or otherwise protected information appropriately.
- Users will be required to declare any known conflict of interest.
- Where a job function may allow fraud or major theft the function may be controlled by at least two people. Where necessary, attention will be paid to segregation of duties.
- A nominated individual will retain distribution lists for information and ensure that distribution of information is kept to a minimum. Lists will be periodically reviewed to confirm that outputs are still required and with clear marking of information and media for the attention of authorised recipients.
- Audit trails to allow the tracing of all transactions in a system to be held for audit purposes as appropriate. The manager with responsibility will determine the retention period for the audit trail and this will be included in the system security policy or system documentation.

5.6.2 Input Preparation and Validation

All operational systems should have controls to ensure the completeness, accuracy and validity of information processed by electronic or manual systems. These may include: -

Monitoring data received: -

- Stamp and count / sorting, batching or totalling documents
- Online validation of file number, sender, batch and control totals.

- Information received by disk; record confirmation of receipt, view totals and file header details.
- Information by telephone record details and ask for written confirmation where appropriate.
- Information by fax or email will have a named recipient and will be printed, logged, signed off, and filed as required.
- There will be up-to-date and accurate form design to facilitate input and authorisation process.
- Preparation and input will be timely.
- Procedures for handling errors in source information will be defined.
- Pre-input checks may include totals, name and address and date of birth. Manual documents may be signed and input will carry the input user-id. Process documents and file as appropriate, input or manual processes may be verified by a second person.

Dual Input or other input checks to detect the following errors
- Out of range values
- Invalid characters in data fields
- Missing or incomplete data
- Exceeding upper and lower data volume limits
- Unauthorised or inconsistent control data

Also consider the following controls
- Periodic review of the content of key fields or data files to confirm their validity and integrity
- Inspecting hard copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized)
- Procedures for responding to validation errors
- Procedures for testing the plausibility of the input data

5.6.3 Control of Internal Processing
Validation should be incorporated into systems to detect data corrupted by processing errors or through deliberate acts.

Applications software design should assure data integrity.

Applications support staff should be aware of
- Use and location in programs of add and delete functions to implement changes to data
- Running order of programs and program dependency
- Recovery and re-run procedures; and communication with users to confirm successful recovery of data.

5.6.4 Checks and Controls

Required controls will depend upon the nature of the application and the business impact of any corruption of data. Checks that can be incorporated include the following: -

- Session or batch controls, to reconcile data file balances after transaction updates
- Balancing controls, to check opening balances against previous closing balances, namely:
    - Run to run control totals
    - File update totals
    - Program to program controls
- Checks on the integrity of data or software downloaded or uploaded, between central and remote computers
- Hash totals of records or files
- Checks to ensure that application programs are run at the right times
- Checks to ensure that programs are run in the correct order and terminate in case of failure; and where appropriate that further processing is halted until the problem is resolved.
- Documented backup, archiving, recovery and housekeeping procedures exist.

5.6.5 Validation of Outputs

System generated data should be validated. Systems are constructed on the premise that having undertaken appropriate validation, verification and testing the output will always be correct but this is not always the case.

Output validation may include: -

- Plausibility checks to test whether the output is reasonable
- Reconciliation control counts to ensure processing of all data
- Reconciliation across modules and systems where appropriate.
- Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision and classification of the information
- Procedures for responding to output validation tests
- Individual responsibility for unprocessed inputs should be defined and monitoring and prioritisation of these take place

Access to outputs will be restricted physically and logically to authorised people and appropriately reviewed.

Outputs may include management reports, error reports and control reports. Reports may be date stamped and signed off as appropriate.

Errors in manual systems will be corrected as soon as they are detected. Rejected data will be rejected from the system with a helpful message and with error correction at the source of input as soon as it is detected. Error processing should include evidence that all errors are accounted for and may require control

procedures, re-input, or manual processing validation and verification. Correction and resubmission of errors must be approved.

Where necessary, information errors will be returned to the sender/ supplier with reasons for the rejection.

If incomplete data is processed to meet a specific business purpose, with the intent to accept a resubmission at a later date, all users of the system must be informed of the status of the data held.

Authorisation or verification by management will accompany input of reference data or sensitive data (e.g. tax codes for staff). Documents will be signed and dated as input where necessary and, where signature checking is required, a list of authorised signatories to be held securely and readily available to the user.

5.7 Business Continuity Management (Disaster Recovery and Contingency)

The continuity of systems and business processes will be assured by incorporating resilience and by disaster recovery and contingency planning.

Supporting Activities
An organisation wide business continuity plan (Ref. IT Services Recovery Plan) and testing schedule, to maintain critical information processes and services is presented to the Trust JISC in compliance with the Security Standard and the NHS Information Security Management Code of Practice.

The Trust wide business continuity strategy and plan will risk assess all business processes including those specific to information security and links to the IT Services Recovery Plan will be made via the Trust IG Lead.

IT Services Recovery Plan maintenance will include

- Identification of events that can cause interruptions to business processes affecting information security (e.g. equipment failure, flood, fire leading to loss of a building or the network for example). Events may affect one or many LLR organisations such that the IT Services Recovery Plan must be considered across Leicestershire and Rutland to ensure that counter-measures are determined and are not limited by organisation boundaries.
- An assessment of how long users could manage without each computer system; an assessment of the criticality of each system; impact of disruption to services in the short medium and long term.
- Assessment of how resilience and continuity will be achieved including
    - Emergency procedures describing the immediate actions to be taken following a major incident which jeopardises business operations or human life. These should be co-ordinated with Risk Management emergency planning procedures.
    - Fall back procedures for both short term and long term loss, which describe the action to be taken to transfer to a manual system and/ or to move essential business activities or support services and staff to alternative temporary locations.
    - Resumption procedures describing the actions to be taken to return to normal full operations, usually at the original site.
    - A test schedule, which describes to what extent and when the plan will be tested.
- Key personnel and responsibilities in the event of disruption occurring.
- Key suppliers
- Method of invoking the plan
- Reporting structures
- Establishment of command centre
- Inventories
- Press and media relations

- Emergency services contact points
- Off-site storage
- Identification and handling of vital records
- Details of agreed procedures and processes
- Insurance requirements

Plan maintenance and scheduled testing will be agreed with the Trust IG Lead and LHIS ISM to provide assurance to the JISC.

The manager with responsibility (IAA/IAO) will ensure that continuity and contingency plans are reviewed and/ or tested on at least an annual basis and that there is appropriate education in agreed emergency procedures and processes. Any change to the business continuity plan must be done under formal change control procedures. System reviews, will take account of trends in usage, particularly in relation to business applications or management information, to enable assessment of future capacity requirements and consequent impact on systems, including the network.

APPENDIX

CONTACT LIST			
NAME	TITLE	TEL	EMAIL
Daljit Kaur Bains	Data Protection Contact		
Mandy Ashton	Caldicott Guardian		
	Local Counter Fraud Specialist NHS Fraud and Corruption line	08702 400 100	

Glossary of Terms

Information Security Forum: British Standard requires organisations to have a cross functional forum for consideration of information security. In organisations served by HIS, this is represented by an IM&T group or equivalent, which is normally chaired by the Director with responsibility for IM&T.

Patient-identifiable and other sensitive information. This phrase concerns patient-identifiable information, confidential staff information, and business sensitive details.

Hardware - Equipment concerning or connected to a computer is often referred to as hardware. This equipment is divided into two categories, hardware and peripherals. Hardware is the heart of any computer system enabling the processing and storing of electronic data. Hardware includes:

- The base or tower unit of PC's – normally containing the processor and hard disk drive
- Notebook or Laptop computers
- Network servers
- Removable or External Hard disk or Zip drives
- Removable or External Tape drives.
- Any other removable data storage devices

- PDA's (see below)

PDA - Personal Digital Assistant. Any electronic device capable of creating, receiving, transmitting and storing portable data with the ability to connect to and exchange information with a PC or laptop computer. This includes devices known as:

- Palm Tops
- Hand Held computers
- Psions
- Some mobile phones
- Any other make/type of equipment meeting this criterion.

Media - Removable digital, laser, magnetic, optical or paper based **information store**. Examples include:

- Medical records
- Letters, documents, computer print-outs
- Floppy disks
- Magnetic Tape – (incl. Audio, computer and video)
- CD-R + CD-RW
- Optical Disks
- Zip drive cassettes

Software - Programs loaded onto hardware may enable the user to create, process and store information. Software may require a licence. Software includes the operating system, Microsoft Windows and application suites such as Microsoft Office, which comprises Access, Excel, Outlook, PowerPoint and Word.

Peripherals - Equipment connecting to hardware to enable input and output of electronic data. Peripherals are often interchangeable. They do not store data. Peripherals include:

- Monitor
- Keyboard
- Mouse/Trackball
- Scanner

- Printer
- Projector

Firewall - A Firewall is security mechanism that limits access across a network connection.