The Queen Elizabeth Hospital
King's Lynn
NHS Foundation Trust

INFORMATION SECURITY POLICY

Unique Reference / Version				
Primary Intranet Location	**Policy Name**	**Version Number**	**Next Review month**	**Next review year**
Information Management & Governance	**Information Security Policy**	**3.0**	**November**	**2014**
Secondary Intranet Location				

Current Author	Mike West
Author's Job Title	Head of ICT
Department	ICT
Ratifying Committee	Information Governance Committee
Ratified Date	2nd November 2012
Review Date	November 2014
Owner	Barbara Cummings
Owner's Job Title	Director of Planning & Performance

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet

Related Policies	Access to Health Records Policy Data Encryption Policy Data Network Security Policy Disposal of IT Equipment and Media Policy Information Governance Policy Internet and Email Acceptable Use Policy Mobile Computing Policy Management of Adverse Events and Serious Incidents Policy Network Security Policy Registration Authority Operational Policy and Procedure Remote Access (External Organisations) Policy Social Media Policy

Stakeholders	Information Governance Committee Non-Clinical Governance Committee

Version	Date	Author	Author's Job Title	Changes
V2	May 2010	Mike West	Head of ICT	
V3	October 2012	Mike West/Phil Cottis	Head of ICT / IG & RA Manager	Review

Short Description

The purpose of this policy is to ensure that:

- The Trust's information systems are properly assessed for security;
- Confidentiality, integrity and availability are maintained;
- Staff are aware of their responsibilities, roles and accountability; and
- Procedures to detect and resolve security breaches are in place.

Key words

Information, Security, Network, Access Control, Incident, Risk, Disaster Recovery, Email, Internet.

INFORMATION SECURITY POLICY

CONTENTS

INFORMATION SECURITY POLICY

1 INTRODUCTION

1.1 Data stored in information systems represents an increasingly valuable asset to the Trust as systems proliferate and increased reliance is placed on them.

1.2 The Trust seeks to protect its information systems from misuse and to minimise the impact of service breaks by developing this Information Security Policy and procedures to manage and enforce it.

1.3 The key issues addressed by this policy are:

- **Confidentiality**: Data access is confined to those with specified authority to view the data;
- **Integrity**: All system assets are operating correctly according to specification and in the way the current user believes them to be operating; and
- **Availability**: Information is delivered to the right person when it is needed.

2 PURPOSE

2.1 The purpose of the policy is to ensure that:

- The Trust's information systems are properly assessed for security;
- Confidentiality, integrity and availability are maintained;
- Staff are aware of their responsibilities, roles and accountability; and
- Procedures to detect and resolve security breaches are in place.

3 DEFINITIONS

3.1 **Asset**
Anything that has value to the organisation, its business operations and its continuity.

3.2 **Availability**
The property of being accessible and usable upon demand by an authorised entity.

3.3 **Confidentiality**
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

3.4 **Information Security**
The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

3.5 **Information Security Management System (ISMS)**
That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

3.6 **Integrity**
The property of safeguarding the accuracy and completeness of assets.

3.7 **ISO/IEC 27001:2005**
The current international specification for the ISMS (superseded BS7799-2:2002).

3.8 **Mitigation**
Limitation of the negative consequence of a particular event.

3.9 **Risk**
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

3.10 **Risk Assessment**
The overall process of risk analysis and risk evaluation.

3.11 **Risk Management**
The process of co-ordinating activities to direct and control an organisation with regard to risk.

3.12 **Statement of Applicability**
A document describing the control objectives and controls that are relevant and applicable to the organisation's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.

3.13 **SIRO**
Senior Information Risk Owner

4 RESPONSIBILITIES

4.1 **Chief Executive**
The Chief Executive has ultimate responsibility for information security, both policy and implementation, within the Trust. The overall responsibility is delegated to the Director of Non-Clinical Services and Performance Management.

4.2 **Director of Non-Clinical Services and Performance Management**
The Director of Non-Clinical Services and Performance Management is responsible for:

- Making arrangements for information security by setting an overall information security policy for the Trust;
- Allocating responsibilities for the management of Information Security; and
- Ensuring that, where appropriate, staff receive information security awareness training.

4.3 **Head of ICT**
The Head of ICT is responsible for the implementation and enforcement of the Information Security Policy, and has responsibility for:

- Monitoring and reporting on the state of information security within the Trust;
- Ensuring that the Information Security Policy is implemented throughout the

Trust;

- Developing and enforcing detailed procedures to maintain security;
- Ensuring compliance with relevant legislation;
- Ensuring that the Trust's personnel are aware of their responsibilities and accountability for information security; and
- Monitoring for actual or potential IM&T security breaches.

4.4 **Information Governance & RA Manager**

The Information Governance and RA Manager is the designated Information Security Officer for the Trust and has responsibility for:

- Acting as point of contact on information security for both staff and external organisations;
- Implementing an effective framework for the management of security;
- Advising on the content and implementation of the information security programme;
- Co-ordinating the production of organisational standards, procedures and guidance on information security matters; and
- The development and implementation of the Information Security Management System to work towards compliance with the requirements of BS ISO/IEC 27001.

4.5 **Caldicott Guardian**

The Caldicott Guardian is responsible for ensuring that the Caldicott principles for the handling of patient identifiable data are adhered to in relation to all Information systems both manual and automated.

4.6 **Information Governance Committee**

The Information Governance Committee will promote information security by:

- Implementing the Information Security Policy throughout the Trust;
- Ensuring awareness of all employees' accountabilities and responsibilities.
- Reviewing and authorising information security policies and responsibilities;
- Reviewing incident reports relating to security and ensure appropriate action is taken to reduce or eliminate risk; and
- Developing and enforcing Trust information security.

4.7 **Auditors**

This policy, its implementation and systems will be subject to periodic review by both internal and external auditors, the recommendations from which will normally be implemented unless specific dispensation is given at Trust management level. Any major security incident will be referred to the auditors and HR, for investigation, disciplinary action will be taken if appropriate.

4.8 **Managers**

Trust Management are directly responsible for:

- Ensuring that all current and future staff are instructed in their security responsibilities;

- Ensuring that all their staff using information systems/media are trained in their use;
- Ensuring that no unauthorised staff are allowed to access any of the Trust's information systems as such access could compromise data integrity;
- Determining which individuals are to be given authority to access specific information systems. The level of access to specific systems should be on a job function need, independent of status;
- Implementing procedures to minimise the Trust's exposure to fraud/theft/disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas;
- Ensuring that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability;
- Ensuring that staff are aware of the Trust's Corporate and Information Governance Frameworks;
- Ensuring that all staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment;
- Ensuring that the relevant systems managers are advised immediately about staff changes affecting computer access (eg job function changes/leaving department or organisation) so that passwords may be withdrawn/deleted;
- Ensuring that any actual or potential breach of information security policy within their area of responsibility is reported via the Trust incident reporting system (Datix).

4.9 **Staff**

All employees and anyone working on behalf of the Trust, involved in the receipt, handling or communication of information, must adhere to this policy to support the reputation of the Trust and where relevant of their profession.

Each employee will be personally responsible for ensuring that no breaches of hardware or software security result from their actions.

Each employee should declare any potential conflicts of interest as required by the Trust's Standing Orders

4.10 **National management**

The NHS Connecting for Health Information Governance Programme has responsibility for ensuring that the NHS is able to effectively manage risks associated with the use of information systems and networks.

4.11 **N3**

The process of connection to N3 is co-ordinated through the Connecting for Health program.

The Trust will adhere to the N3 Data Security Policy and has signed the Code of Connection. Security measures apply to all systems and users connected to the Trust's local area network.

5 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

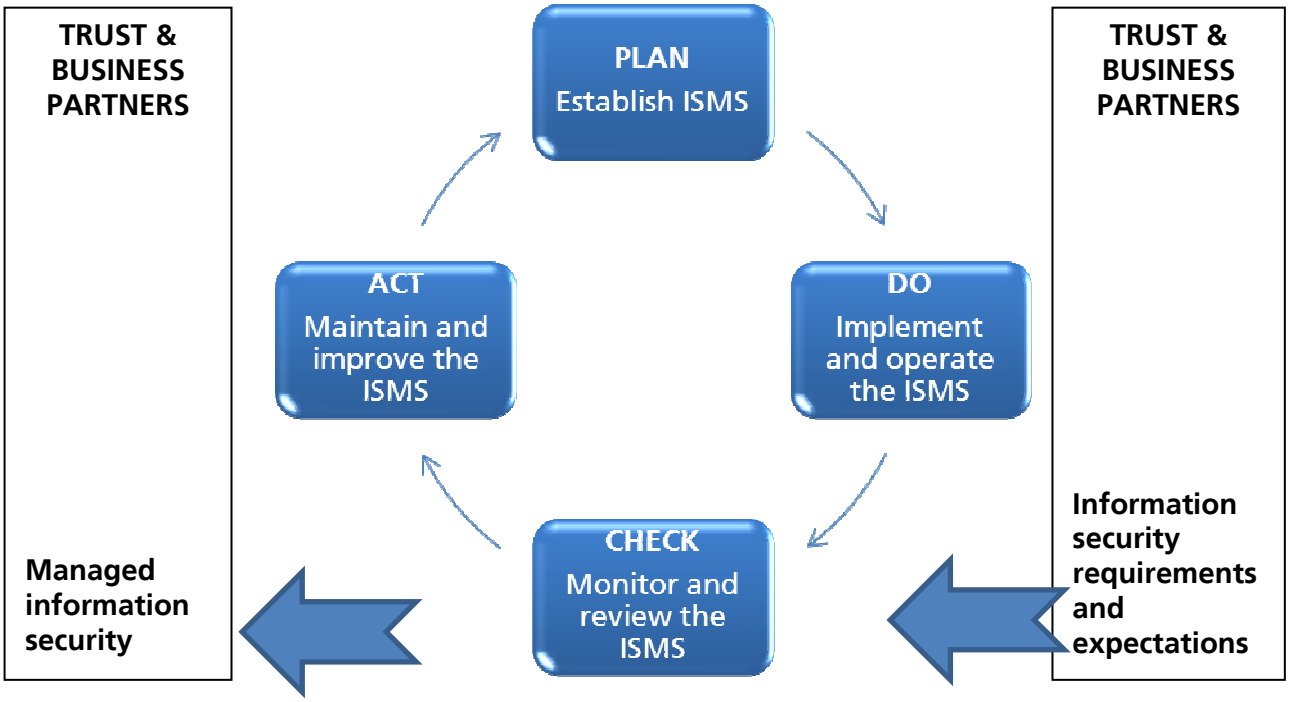
5.1 Although the Department of Health's Information Governance Toolkit provides the basis of the ISMS that supports a foundation level of information security, the Trust is fully committed to the goals and principles of information security and to manage information security effectively an Information Security Management System (ISMS) will be developed to provide a framework for information security. Owners will be identified for specific information systems and, where appropriate, specific datasets. These owners will work with the Caldicott Guardian to determine appropriate data sharing protocols, access protocols and appropriate security practices and procedures.

5.2 Effective information security involves more than simply installing a security product, implementing anti-malware software, providing a security policy or signing a contract with a support service provider. The ISMS, therefore, provides a means to identify and co-ordinate the approach to the management of information security by the Trust in order to protect it and its business partners.

5.3 The process adopted by the Trust reflects the requirements of ISO 27001 by emphasising the importance of:

- Understanding the Trust's information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage information security risks in the context of the Trust's overall business risks;
- Monitoring and reviewing the performance and effectiveness of the ISMS; and
- Continual improvement based on objective measurement.

5.4 The Trust has also adopted the 'Plan-Do-Check-Act' (PDCA) model, which is applied to structure all ISMS processes. The figure below illustrates how a ISMS takes as input the information security requirements and expectations of the Trust and its business partners and through the necessary actions and processes produces information security outcomes that meet those requirements and expectations.



6 RISK MANAGEMENT

6.1 Objective

6.1.1 To identify and counter possible threats to the security policy and standards.

6.2 Methodology

6.2.1 All systems will be subject to periodic security reviews by systems managers. The depth of a review will be determined by the importance and size of the particular system.

6.2.2 Individual systems should be periodically reviewed. A rolling program will be formulated by the ICT Department and agreed with Internal Audit.

Reviews will include:

- Identification of assets of the system;
- Evaluation of potential risks/threats;
- Assessment of likelihood of threats occurring;
- Identification of practical cost effective counter measures. These must be included in the Trust's Business Continuity Plans; and
- Implementation programme for counter measures (contingency plans).

6.2.3 Systems are liable to independent reviews by internal and external auditors.

6.3 Reporting

6.3.1 Each system review will include a formal report to the Trust's Executive Board (TEB) containing findings and recommendations.

7 EQUIPMENT SECURITY

7.1 Objective

7.1.1 To protect IM&T equipment against loss or damage and avoid interruption to business activity.

7.2 Equipment Siting and Protection

7.2.1 IM&T equipment will always be installed and sited in accordance with the manufacturer's specification.

7.2.2 Environmental controls will be installed to protect central/key equipment. Such controls will trigger alarms if environmental problems occur. In such cases only authorised entry will be permitted.

7.2.3 Smoking, drinking and eating is not allowed in areas housing central/key computer equipment and doors should be kept locked at all times. Individual users should not

consume food or drink adjacent to sensitive computer equipment.

7.3 Power Supplies

7.3.1 The Trust has generator backup power to the mains electricity supply. The Estates Department will carry out regular checks of the backup power systems and the UPS are also tested at this time.

7.3.2 Critical computer equipment will be fitted with battery back-up to ensure that it does not fail during switchovers between mains and generator. Such battery power should suffice for at least 10 minutes at normal usage.

7.4 Cable Routing

7.4.1 All cabling (electricity or communications) between buildings will be via underground conduit and not accessible to unauthorised people where this is feasible and financially viable.

7.4.2 All cabling within buildings will be in steel conduits and work will be undertaken by the Estates Department or a Trust approved contractor.

7.5 Equipment Maintenance

7.5.1 All central processing equipment, including file servers, will be covered by third party maintenance agreements.

7.5.2 All personal computers, terminals and printers will be covered by maintenance agreements with third parties for repair of out of warranty equipment provided it is cost effective (each case will be judged on its merits). All such repairs will only be made on approval by the ICT department.

7.5.3 All such third parties will be required to sign confidentially agreements.

7.5.4 Records of all faults/suspected faults will be maintained on the ICT helpdesk system.

7.6 Remote Diagnostic Services

7.6.1 Suppliers of central systems/software expect to have remote access to such systems on request to investigate/fix faults. The Trust will permit such access subject to this either being an N3 connection or a connection made through the Trusts strong authenticated Remote Access Server. All activity will be monitored.

7.6.2 Each supplier requiring remote access will be required to sign a remote access agreement requiring confidentiality of data/information by qualified representatives.

7.6.3 To prevent the possibility of unauthorised access - modem links will NOT be connected under any circumstances. The only authorised route using a modem to access the Trusts servers or network is via the Trusts remote access server.

7.7 Security of Hard Disks

7.7.1 Hard disks on any machine may contain sensitive/confidential data. Removal off site of faulty disks represents a potential threat to the Trust. Each such case will be judged on its merits balancing the need versus the risk of breach of confidentiality and then only to approved repairers who will have signed confidentiality agreements. Whenever possible the data and information should be overwritten or the equipment de-gaussed. Obsolete or faulty Hard Drives and Tapes will be disposed of in a confidential manner (see the Trust's Disposal of IT Equipment and Media Policy).

7.8 Security of Equipment Off Premises

7.8.1 Equipment and data will not be taken off site without formal approval, other than to transport it from one of the Trust's sites to another. (See the Trusts Mobile Computing Policy)

7.9 Mobile Data Devices

7.9.1 Refer to the Trust's Mobile Computing Policy and Data Encryption Policy.

7.10 Disposal of Equipment

7.10.1 Computer hardware disposal can only be authorised by the ICT department. They will ensure that data storage devices are purged of sensitive data before disposal or securely destroyed in accordance with the documented procedures.

7.10.2 Unusable computer media should be destroyed (e.g. floppy disks, magnetic tapes, CD-ROMS) in accordance with the documented disposal procedures.

8 ACCESS CONTROLS

8.1 Objectives

8.1.1
- To identify the location of the Trusts Information systems assets
- To identify and authorise the use to which such assets are put
- To manage capital charges on physical assets

7.2 Physical Assets

8.2.1 An up to date register of acquisitions and disposals of physical computer assets will be maintained, this will include the location, Department and serial number. The Facilities Department will maintain this asset register.

8.3 Software

8.3.1 It is the responsibility of the ICT Department to hold licences for all software loaded on Trust computer systems.. Trust approved software will only be supported by the

ICT Department. Any software procurement will only take place after approval of the Head of ICT or appropriate deputy.

8.4 System Ownership

8.4.1 Each of the Trust's central and Departmental software applications will be the responsibility of a specified application manager whose responsibilities will include ensuring compliance with the Trust's Information Security Policy, ensuring the appropriate use of the equipment, troubleshooting and maintenance of the software application. The ICT department will assist system managers with this task.

8.4.2 The ICT department will be responsible for all the Trust's computing platforms, including maintenance, operating system and network infrastructure support.

9 ACCESS CONTROL TO SECURE AREAS

9.1 Objective

9.1.1 To minimise the threat to the Trust's information systems through damage or interference.

9.2 Physical Security

9.2.1 All central processors/networked file servers/central network equipment will always be located in secure areas with restricted access.

9.2.2 The Trust's central computer rooms will be high security areas housing the Trusts Corporate and Departmental multi user systems. An entry restriction system will be incorporated to protect the suite. The Trusts swipe card entry restrictions will be applied. Access logs will be received by the ICT Department and reviewed weekly.

9.2.3 Local network equipment/file servers and N3 terminating equipment will always be located in secure areas and/or lockable cabinets.

9.3 Entry Controls

9.3.1 Unrestricted access to the central computer facilities will be confined to designated staff, whose job function requires access to that particular area/equipment. Restricted access to other staff, where there is a specific job function need for such access, will be granted on a temporary basis.

9.3.2 Authenticated representatives of third party support agencies will only be given access through specific authorisation from the SIRO or appropriate deputy.

9.3.3 Logs will be maintained of pass card entry to the Computer rooms via the Trust's Building Management System. A further visitors log is maintained in each of the Computer rooms detailing the name, date, company and reason for visit of all visitors to the rooms.

10 SECURITY OF THIRD PARTY ACCESS

10.1 Objective

10.1.1 To enable the Trust to control external access to its systems.

10.2 Access Control

10.2.1 No external agency (NHS or not) will be given access to any of the Trust's networks unless that body has been formally authorised to have access. All non NHS agencies will be required to sign security and confidentiality agreements with the Trust.

10.2.2 External agencies will only be allowed access to specific/relevant systems.

10.2.3 The Trust will control all external agencies access to its systems, either using the strong authenticated Remote Access Server or access via N3 for organisations that have full code of connection.

10.2.4 Refer to the Trust's Remote Access (External Organisations) Policy.

10.3 N3 requirements

10.3.1 Strong authentication procedures/technology has been introduced for ALL remote connections to the Trust's computer systems where concurrent connection to the N3 is not possible.

10.3.2 The Trust requires that third parties providing remote support do so over N3 wherever possible. Where this is not possible then modem access using strong authentication/VPN via the Trusts remote access server should be used as an alternative.

11 USER ACCESS CONTROL

11.1 Objective

11.1.1 To control individual's access to systems to that required by their job function.

11.2 Registering Users

11.2.1 Formal procedures will be used to control access to systems. An authorised manager should countersign each application for access.

11.2.2 Access privileges will be modified/removed - as appropriate - when an individual changes job/leaves.

11.2.3 For nationally hosted systems installed as part of the Connecting for Health programme refer to the Trust's Registration Authority Operational Policy and Procedure.

11.3 User Password Management

11.3.1 No individual will be given access to a live system unless properly trained and made aware of their security responsibilities.

11.3.2 Users should keep their passwords secret and never disclose them to colleagues.

11.3.3 Passwords should be changed regularly - all new systems will include password ageing to force users to change their password periodically. The recommendation of ISO 27000 is that all passwords should be changed every 30 days. The current Trust systems have expiry dates ranging from 30 to 90 days expiry. Windows Domain Passwords will be complex 8 characters, including a combination of upper and lowercase letters and numbers.

11.3.4 Users with authorised access to more than one system may have the same password on all systems to which they have access. This may give different access privileges on different systems depending on job need.

12 SECURITY INCIDENT MANAGEMENT

12.1 Objective

12.1.1 To detect, investigate and resolve any suspected/actual information system security breach.

12.2 Security Incidents

12.2.1 A security incident is an event that may result in one or more of the following:

- Degraded system integrity;
- Loss of system availability;
- Disclosure of confidential information;
- Disruption of activity;
- Financial loss;
- Legal action; and
- Unauthorised access to applications.

12.2.2 All instances of incidents involving the mismanagement of information should be reported through the Trust's electronic Incident Reporting System (Datix). These will then be passed to the SIRO, Caldicott Guardian or Information Governance & RA Manager for further investigation as appropriate.

12.2.3 Information Security breaches may result in disciplinary action.

12.3 Individual's Responsibilities

12.3.1 Each information user is personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

12.3.2 Computer users should ensure that they do not disclose their passwords or allow anyone else to use their password or allow another user to work under their log on.

Passwords that have potentially been compromised should be changed by the user immediately.

13 HOUSEKEEPING

13.1 Objective

13.1.1 To maintain the integrity and availability of computer assets.

13.2 Data Backup

13.2.1 All central systems will have daily backup regimes formalised. Such backups will have a minimum of a 5 day cycle before media is overwritten. Removable backup media will be kept in a secure location in a separate fire zone away from the Servers concerned.

13.2.2 The viability of central systems backups will be provided when used in contingency tests.

13.3 Incident Reporting

13.3.1 All the Trust's central systems will have formal incident recording and escalation procedures.

13.3.2 Incident recording will be used to log all unusual events. This mechanism will include what happened, what was done and final resolution.

13.3.3 Major incident control procedures will be used to manage serious problems e.g., inability to recover critical live systems.

13.4 Media Disposal

13.4.1 To ensure data confidentiality all obsolete removable media will be disposed of via the ICT department who will arrange appropriate confidential disposal and destruction (refer to Trust's Disposal of IT Equipment and Media Policy).

14 DATA VALIDATION

14.1 Objective

14.1.1 To maintain confidence in data accuracy for use in decision making.

14.2 At Data Input

14.2.1 Data accuracy is the direct responsibility of the person inputting the data supported by their line manager.

14.2.2 All systems will include validation processes at data input to check in full or in part the acceptability of the data. Depending on the system, later validation may be necessary to maintain referential integrity.

14.2.3 Systems should report all errors together with a helpful reason for the rejection to facilitate correction.

14.2.4 Error correction should be done at the source of input as soon as it is detected. Such correction is increasingly important as systems are linked and errors can be transmitted between systems.

14.2.5 Any loss or corruption of data should be reported to the relevant system manager at once - this should involve incident recording mechanisms immediately and possibly major incident control (dependant on the severity of the problem).

14.3 Internal Validation

13.3.1 All systems will incorporate internal validation processes and audit trails to detect and record problems with processing/data integrity.

15 SOFTWARE PROTECTION

15.1 Objective

15.1.1 To comply with the law on licensed products and minimise risk of computer viruses.

15.2 Licensed Software

15.2.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. The ICT Department will be responsible for holding copies of all licences.

15.3 Trust Software Standards

15.3.1 The Trust will only permit approved software to be installed on its PCs. Approval will be via the ICT department. The Head of ICT (or designated deputy) will countersign all requisitions for new software.

15.3.2 The Trust will require the use of specific general purpose packages (e.g., word-processing, spreadsheets, databases) to facilitate support and staff mobility. Non approved packages should be phased out as soon as practicable - these cannot be supported by the ICT Department.

15.3.3 Where the Trust recognises the need for specific specialised PC products, such products should be approved and registered with the ICT department and be fully licensed.

15.3.4 Shareware programs are only free when under evaluation. Full licences should be purchased if the program is used on Trust business. Freeware is totally free, but all Users should seek guidance from the ICT Department on the correct use of both Shareware and Freeware.

15.3.5 Users should not load any software onto Trust PCs without the prior approval of the

ICT Department.

15.4 Virus Control

15.4.1 The Trust seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software loaded on all Networked PCs and Servers.

15.5.2 Users should report any viruses detected/suspected on their machines immediately to the ICT Helpdesk.

15.5.3 No newly acquired disks/CDs from whatever source are to be loaded unless they have previously been virus checked by the locally installed virus checking package. USB drives and other portable media must also be scanned for viruses prior to use.

15.5.4 The ICT Department will be responsible for installing and updating the Anti-Virus software. Virus databases will be updated on a regular basis and all networked systems and users will be protected. Virus software will also be loaded on standalone PC's. All devices connected to the Trust network will automatically have anti-virus software loaded. Definition files will also be updated at least daily.

15.5 Private Use

15.5.1 Private use of Trust Hardware and Software is permitted provided that it is not for personal gain, not at Trust expense and is undertaken in the employee's own time.

16 DATA NETWORK SECURITY

16.1 Objective

16.1.1 To be able to ensure the security of the Trust's Data Network. To do this the Trust will:

- Ensure availability;
- Ensure that the network is for authorised users;
- Preserve the integrity of all data and information on the network;
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the Trust's assets;
- Preserve confidentiality; and
- Protect against unauthorised disclosure.

16.1.2 For further information refer to the Trust's Network Security Policy.

16.2 Data Network Definition

16.2.1 The Data Network is a collection of communication equipment such as LAN switches, routers, servers, computers, printers, which have been connected together. The network is created to share data, software and peripherals such as printers, fax machines, internet/email connections, hard disks and other storage

equipment.

16.3 Network Security Policy

16.3.1 This policy applies to all networks with the Trust used for;

- The storage, sharing and transmission of non-clinical data and images;
- The storage, sharing and transmission of clinical data and images;
- Printing or scanning non-clinical or clinical data or images; and
- The provision of Internet and email systems for receiving, sending and storing non-clinical and clinical data or images.

16.3.2 To satisfy this the Trust will undertake the following;

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures;
- Provide both effective and cost-effective protection commensurate with the risks to its network assets;
- Implement the Network Security Policy in a consistent, timely and cost effective manner; and
- Where relevant the Trust will comply with the following legislation:
  - Access to Health Records Act1990;
  - Computer Misuse Act 1990;
  - Copyright, Design and Patents Act 1998;
  - Data Protection Act 1998;
  - Electronic Communication Act 2000;
  - Freedom of Information Act 2000;
  - Health and Social Care Act 2001; and
  - Human Rights Act 1998.

17 DISASTER/RECOVERY PLANNING

17.1 Objective

17.1.1 To be able to restore computer facilities to maintain essential business activities following a major failure or disaster.

17.2 Need for Effective Plans

17.2.1 The Trust recognises that some form of disaster may occur, despite precautions, and therefore seeks to contain the impact of such an event on its core business through tested disaster recovery plans.

17.2.2 The Trust recognises that IM&T systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms.

17.3 Planning Process

17.3.1 The main elements of this process will include:

- Identification of critical computer systems;
- Identification and prioritisation of key users/user areas;
- Agreement with users to identify disaster scenarios and what levels of disaster recovery are required;
- Identification of areas of greatest vulnerability based on risk assessment;
- Mitigation of risks by developing resilience; and
- Developing, documenting and testing disaster recovery plans identifying tasks, agreeing responsibilities and defining priorities.

17.4 Planning framework

17.4.1 Disaster recovery plans will cater for different levels of incident including:

- Loss of key user area within a building;
- Loss of a key building;
- Loss of key part of computer network; and
- Loss of processing power.

17.4.2 Disaster recovery plans will always include: -

- Emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel);
- Fallback procedures describing the actions to be taken to provide contingency devices defined in the disaster recovery plan;
- Resumption procedures describing the actions to be taken to return to full normal service; and
- Testing procedures describing how the disaster recovery plan will be tested.

18 EMAIL AND INTERNET

18.1 Objective

18.1.1 To control and monitor the use of email and the Internet. To protect the Trust and the users from misuse.

18.2 User Agreements

18.2.1 Users of the Trusts Email system and connection to the N3 and the Internet will be given a copy of the Trust's Internet and Email Acceptable Use Policy. New accounts will not be enabled until the user signs and returns the acknowledgement slip to the ICT department.

18.3 Protecting Personal Use During Absence – The 'Email Deputy' System

18.3.1 There may be occasions when it is necessary for the Trust to access an individual's email account in their absence, in order to continue efficient operations within the organisation (e.g. where the individual has not had an opportunity to set up an 'out of office' message or redirect their email due to unplanned absence).

18.4 Further Guidance

18.4.1 For further details refer to the Trust's Internet and Email Acceptable User Policy and Social Media Policy.

19 EQUALITY IMPACT ASSESSMENT

19.1 A Stage 1 (Screening) - Equality Impact Assessment has been undertaken and no negative impact on any group was indicated (see Appendix 2).

20 DISSEMINATION OF DOCUMENT

20.1 Following approval by the Information Governance Committee, this policy will be submitted to the Non-Clinical Governance Committee for information. This policy will be uploaded onto the Trust intranet site under ICT and on the Information Governance intranet page. Policy notification will be through an email to the Management Forum and through the Information Governance Newsletter. See Appendix 3 for details.

20.2 All departmental heads / ward managers will be supported by the Information Governance & RA Manager.

21 REFERENCES

21.1 References to Standards

- BS ISO/IEC 27001, British Standards for Information Security
- Caldicott Report (December 1997)
- Information Governance Toolkit v.10

21.2 Legislation

- Access to Health Records Act1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1998
- Data Protection Act 1998
- Electronic Communication Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2001
- Human Rights Act 1998

21.3 **Guidance**

- Ensuring Security and Confidentiality in NHS Organisations (E5498)
- Information Security Management: NHS Code of Practice (April 2007)
- NHS Confidentiality Code of Practice (November 2010)

APPENDIX 1 ARRANGEMENTS FOR MONITORING COMPLIANCE WITH THIS POLICY

The compliance with this policy will be monitored by:

Key elements (Minimum Requirements)	Process for Monitoring (e.g. audit)	By Whom (Individual / group /committee)	Frequency of monitoring	Responsible individual / group / committee (plus timescales(for		
				Review of Results	Development of Action Plan	Monitoring of action plan and implementation
Reducing the number of Information Security breaches	Management of incidents relating to Information Governance	Head of Risk Management	Monthly	Information Governance Committee	Relevant Manager according to the issue	Information Governance Committee
Ensuring best practice across the Trust	Undertaking Information Security Audits (as part of Confidentiality Audits)	IG Team	Monthly	Information Governance Committee	IG & RA manager	Information Governance Committee

APPENDIX 2 EQUALITY IMPACT ASSESSMENT

To be completed and attached to any policy document when submitted to the appropriate committee for ratification

STAGE 1 - SCREENING

Name & Job Title of Assessor: Mike West, Head of ICT			**Date of Initial Screening: 07/05/10**
Policy or Function to be assessed: Information Security Policy			
		Yes/No	**Comments**
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**		
	3.1 Race & Ethnic background	No	This policy is applied equally to all groups
	3.2 Gender including transgender	No	This policy is applied equally to all groups
	3.3 Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	This policy is applied equally to all groups
	3.4 Religion or belief	No	This policy is applied equally to all groups
	3.5 Sexual orientation	No	This policy is applied equally to all groups
	3.6 Age	No	This policy is applied equally to all groups
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	This policy is applied equally to all groups

If the answer to any of the questions above is yes, please complete a full Stage 2 Equality Impact Assessment.

Signature of Assessor: Mike West: Head of ICT **Date: 03.10.12**

Signature of Line Manager: Barbara Cummings: Director of Planning & Performance **Date: 03.10.12**

APPENDIX 3 PLAN FOR DISSEMINATION OF PROCEDURAL DOCUMENTS

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Acknowledgement: University Hospitals of Leicester NHS Trust

Title of document:	**Information Security Policy**		
Date finalised:		**Dissemination lead: Print name and contact details**	**Mike West** **Head of ICT** **mike.west@qehkl.nhs.uk**
Previous document already being used?	**Yes**		
If yes, in what format and where?	**Electronic format on ICT Intranet page & Policies & Procedures: ICT**		
Proposed action to retrieve out of date copies of the document:	**Remove outdated policy from Trust Intranet**		

To be disseminated to:	**How will it be disseminated, who will do it and when?**	**Format**	**Comments:**
All staff	**Policies & Procedures: Information Management & Governance + ICT Intranet page**	**Electronic**	**Trust Staff advised through IG newsletter and email to Management Forum**

Dissemination Record - to be used once document is approved

Date put on register / library of procedural documents:		**Date due to be reviewed:**	

Disseminated to: (either directly or via meetings, etc.)	**Format (i.e. paper or electronic)**	**Date Disseminated:**	**No. of Copies Sent:**	**Contact Details / Comments:**

APPENDIX 4 CHECKLIST FOR THE REVIEW AND APPROVAL OF PROCEDURAL DOCUMENTS

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	**INFORMATION SECURITY POLICY**	
		Yes/No/ Unsure	**Comments**
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is the method described in brief?	Yes	
	Are individuals / stakeholders / users involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	Does the document identify which committee will ratify it?	Yes	
	If appropriate, have the joint Human Resources/staff side committee (or equivalent) approved the document?	NA	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it	Yes	

	Title of document being reviewed:	INFORMATION SECURITY POLICY	
		Yes/No/ Unsure	Comments
	will be held?		
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process for Monitoring Compliance**		
	Are there measurable standards or KPIs to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Mike West	**Date**	25th October 2012
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Barbara Cummings	**Date**	2nd November 2012
Signature			

Acknowledgement: Cambridgeshire and Peterborough Mental Health Partnership NHS Trust