Medway NHS
NHS Foundation Trust

INFORMATION SECURITY POLICY

Edition No:	5.1	**ID Number:**	POLCGR018
Dated:	August 2015	**Review Date:**	July 2019
Document ID:	Policy	**Document Type:**	Corporate
Directorate:	Corporate Affairs	**Category:**	Governance & Risk
Department(s):	Governance		
Author:	Information Governance Manager	**Sponsor:**	Director of Corporate Affairs

Policy Dissemination

Consultation Process
Name of Individuals Consulted
Technical Programmes Manager
Head of Clinical Systems Development

Name of Specialised Committee / Group Consulted
Information Governance Committee – 15th June 2015

Corporate Approval		
Committee Title	Chief Executive Advisory Group	Date: August 2015

Document Control / History	
Edition No	**Reason for change**
1	Bi-annual review and update of policy
2	Review and update of policy
3	Review and update of policy
4	Review and update of policy
5	Review and update of policy – updated reference to ISO 27001:2013. Change of job titles
5.1	Extend review date due to waiting for IT outsourcing consultation to be finalised.

Document	**Ref No**
References:	
Data Protection Act (1998),	
The Copyright Designs & Patents Act (1988)	
Computer Misuse Act (1990),	
Human Rights Act (1998)	
Confidentiality: NHS Code of Practice November 2003	
Information Security Management	ISO/IEC 27001:2013
Information Security Management: NHS Code of Practice April 2007	
Information Governance Tool Kit	
Trust Associated Documents:	
Data Protection Policy	POLCGR007
Information Governance Strategy & Policy	POLCGR017

INFORMATION SECURITY POLICY

Acceptable Use of Trust Information Systems and Assets	POLCGR113
Network Security Policy	POLCGR082
Registration Authority Policy	POLCGR093-1
Remote Access and Working Policy	POLCGR114
Secure Transfer of Information Policy	POLCGR077-1
User Access Management Policy	POLCGR079

Table of Contents

INFORMATION SECURITY POLICY

To be read in conjunction with any policies listed in Trust Associated Documents.

1 INTRODUCTION

1.1 The need for a security policy

Data stored in information systems represents an increasingly valuable asset to Medway NHS Foundation Trust as its systems proliferate and increased reliance is placed on them. The Trust seeks to protect its information systems from misuse and to minimise the impact of Service breaks by developing an Information Security Policy and procedures to manage and enforce it.

2 AIM

2.1 This document is a high-level policy document common to all organisations within Kent & Medway. It provides the context for a supporting set of guidelines and procedures that will determine, at a detailed level, how security and confidentiality is established and maintained for all information, information systems, applications and networks owned or held by Medway NHS Foundation Trust.

2.2 The Trust's policy aims to ensure:

- Computer systems are properly assessed for security
- Confidentiality, integrity and availability are maintained
- Staff are aware of and comply with their responsibilities, roles and accountability
- Information assets are protected
- Procedures to detect and resolve security breaches are in place.

3 OBJECTIVES

3.1 The objectives of the Information Security Policy are to preserve:

Confidentiality - data access is confined to those with specified authority to view the data

Integrity – Information shall be complete and accurate. All system, assets and networks are operating correctly according to specification.

Availability - information is available and delivered to the right person when it is needed.

3.2 The Trust also has legal obligations to maintain security and confidentiality notably under the Data Protection Act (1998), Human Rights Act (1998), Copyright, Designs and Patents Act(1988), and Computer Misuse Act (1990). As well as the common law duty of confidentiality that prohibits use or disclosure of personal information given in confidence, all staff must adhere to the six Caldicott principles (Caldicott Report 1997).

4 SCOPE

4.1 The policy applies to all Trust systems (hardware, software and data) and to all Trust staff, including contractors, services providers, agency workers and other third parties who are currently working under the auspices of the Trust.

5 SECURITY MANAGEMENT

5.1 Objective

5.1.1 To establish the management structure for computer systems security within the Trust.

5.2 Organisational Management

5.2.1 The Information Governance Manager, IT Programmes Manager and Senior Information Risk Owner will jointly act as Information Security Manager for the Trust. They will be responsible for implementation and enforcement of the Information Security Policy and will have organisational security management responsibilities for:

- procedures to detect and resolve security breaches are in place;
- working with Human Resources to develop and implement relevant policies;
- monitoring and reporting on the state of IM&T security within ;
- ensuring the Information Security Policy is implemented throughout the Trust;
- developing and enforcing detailed procedures to maintain security;
- ensuring compliance with relevant legislation;
- ensuring the Trust's personnel are aware of their responsibilities and
- accountability for IM&T security;
- monitoring for actual or potential IM&T security breaches.

Detailed responsibility for particular systems will be delegated to the relevant system managers.

5.3 NHS N3 Network (BS ISO/IEC 27001:2013 – A.13.1)

5.3.1 Organisations are required to adhere to the NHS *net* Security Policy and sign an associated Code of Connection

5.3.2 This may require the implementation of specific security measures. Such security measures will apply to all systems and users connected to the Trust's network.

5.4 NHS Connecting for Health (NHS CFH)) (BS ISO/IEC 27001:2013 – A.13.1)

The NHS Connecting for Health Information Governance Team (IGT) now holds responsibility for the authorisation of all connections and services to and across the N3 network

.

5.5 Auditors (BS ISO/IEC 27001:2013 – A.12.7.1)

The Trust's 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 organisation management level. Any major security incident is liable to be referred to the auditors for investigation

6 SECURITY RESPONSIBILITIES

6.1 Objective (BS ISO/IEC 27001:2013)

6.1.1 To ensure that the Trust's staff are aware of security risks and their responsibilities to minimise the threats.

6.2 **Senior Management responsibilities (BS ISO/IEC 27001:2013 A.6.1.1)**

6.2.1 Ensure all current and future staff are instructed in their security responsibilities;
6.2.2 Ensure all their staff using computer systems/media are trained in their use;
6.2.3 Ensure no unauthorised staff are allowed to access any of the Trust's computer or information systems as such access could compromise data integrity;
6.2.4 Determine which individuals are to be given authority to access specific computer or information systems. The level of access to specific systems should be on a job function need, independent of status;
6.2.5 Implement 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;
6.2.6 Ensure that all new information systems are appropriately authorised and correct procedure followed for procurement.
6.2.7 Ensure current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability;
6.2.8 Ensure staff are aware of the Trust's Standing Orders on potential personal conflicts of interest;
6.2.9 Ensure all staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment;
6.2.10 Ensure the relevant system managers are advised immediately about staff changes affecting computer access (e.g., job function changes or leaving department or organisation) so that passwords may be withdrawn or deleted.

6.3 Caldicott Guardian (BS ISO/IEC 27001:2013 – A6.1.1)

6.3.1 Responsible, on behalf of the Chief Executive, for agreeing, monitoring, and reviewing internal protocols governing access to personally-identifiable information by staff within the organisation, in compliance with UK legislation and national policy and guidance;
6.3.2 Responsible for agreeing, monitoring, and reviewing protocols governing the use of personally-identifiable information across organisations, e.g. with other NHS and local authority services, and other partner organisations contributing to the local provision of care;

6.4 **Senior Information Risk Owner (BS ISO/IEC 27001:2013 – A6.1.1)**

6.4.1 Responsible, on behalf of the Caldicott Guardian, for implementing, monitoring documenting and communicating information security within the organisation, in compliance with UK legislation and national policy and guidance;
6.4.2 Responsible for monitoring and reporting the state of information security within the organisation;
6.4.3 Must have ready access to the Caldicott Guardian for guidance on policy;
6.4.4 Ensure the Information Security Policy is implemented and followed throughout the organisation;
6.4.5 Ensure relevant staff are aware of their security responsibilities and that security awareness training is provided for all users;
6.4.6 Monitor for actual or potential information security breaches within the organisation.

6.5 **Information Governance Manager (BS ISO/IEC 27001:2013 – A.6.1.1)**

6.5.1 Ensure appropriate Data Protection Act notification is maintained for the organisation's systems and information.
6.5.2 Ensure that staff using the systems for which they have responsibility are made aware of the Trust's policy on the handling of confidential data and its disposal.
6.5.3 Responsible for dealing with enquiries about the Data Protection Act, and facilitating staff Subject Access requests;
6.5.4 Responsible for advising users of their responsibilities under the Data Protection Act, including Subject Access;
6.5.5 Responsible for advising the Senior Information Risk Owner on breaches of the Act, and recommending actions;
6.5.6 Responsible for liaising with external organisations on Data Protection Act matters.

6.6 **Head of Clinical Systems Development (BS ISO/IEC 27001:2013 – A.6.1.1)**

6.6.1 Ensure IM&T equipment is sited or protected to reduce risks from environmental threats and hazards, and unauthorised access;
6.6.2 Ensure that data held on systems is backed up on a regular basis (daily, weekly, monthly) depending upon the usage and critical nature of the system. Backups can be of the whole system or only of changes since last backup ('incremental').
6.6.3 Ensure that all backup copies are held either off-site, or in a fire-resistant cabinet suitable for the materials in use.
6.6.4 Staff unsure of the backup procedures for their system contact the IT Programmes Manager who will offer guidance and will assist in setting up a backup/recovery plan.
6.6.5 Ensure IM&T equipment purchases are added to the Trust's inventory, security labelled, appropriate licensed software loaded, and the equipment suitably configured for use;
6.6.6 Must authorise computer hardware disposal, delete it from the Trust's inventory, and ensure data storage devices are purged of sensitive data before disposal or securely destroyed;
6.6.7 Responsible for ensuring that there is a process in place whereby all electronic media and diskettes scheduled for destruction are forwarded to the IM&T department, where the System Support manager will ensure removal of any data and their disposal in accordance with the Trust's Environmental accreditation requirements 14001.
6.6.8 Ensure that all disposals of computer equipment met current National and EU Regulations

6.7 **Kent & Medway HIS Service Desk**

6.7.1 Responsible for allocation and configuration of individual user accounts and associated user authentication for each authorised user of the Trust's network resources and any relevant network operating systems

6.8 **Line Managers (BS ISO/IEC 27001:2013 – A.6.1.1)**

6.8.1 Ensure all current and future staff are instructed in their security responsibilities;
6.8.2 Ensure all their staff using computer systems/media are trained in their use;
6.8.3 Ensure no unauthorised staff is allowed to access any of the Trusts computer or information systems, as such access could compromise data integrity;

6.8.4 Determine which individuals are to be given authority to access specific computer or information systems. The level of access to specific systems should be on a job function need, independent of status;
6.8.5 Implement procedures to minimise exposure to fraud/theft/disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas;
6.8.6 Ensure that all new information systems/procedures meet Trust requirements.
6.8.7 Ensure current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability;
6.8.8 Ensure staff are aware of the Trust's Standing Orders on potential personal conflicts of interest.
6.8.9 Ensure that staff follow the correct procedures for the disposal of printouts containing sensitive patient or staff personal data, which is either by shredding in situ or placed in suitable containers for either incineration or collection by external agents of the Trust assigned with the responsibility for their destruction

6.9 Staff responsibilities (BS ISO/IEC 27001:2013 – A.6.1.1)

6.9.1 Each employed and contracted staff is personally responsible for ensuring that no breaches of computer security result from their actions;
6.9.2 Must comply with the Trust's security policies and procedures. Breaches will be subject to a formal investigation, if found to be deliberate may lead to disciplinary action which may lead to legal action;
6.9.3 All staff are personally responsible for the accuracy and currency of the data they record on systems;
6.9.4 Should declare any potential conflicts of interest as required by the Trust's Standing Orders.
6.9.5 Confidential information should be stored on the network where backups are taken daily.
6.9.6 Where data is held on removable media staff are responsible for ensuring that they are encrypted and stored in a lockable facility.

6.10 Other authorised users (BS ISO/IEC 27001:2013 – A.6.1.1)

6.10.1 Other NHS and authorised external users are personally responsible for ensuring that no breaches of computer security result from their actions;
6.10.2 Must comply with the Trust's security policies and procedures;
6.10.3 Shall have this Policy included as part of a relevant service level agreement or contract.

6.11 System managers (BS ISO/IEC 27001:2013 – A.6.1.1)

6.11.1 Job descriptions for system managers will include specific reference to the security role and responsibility of the post;
6.11.2 All of the Trust's systems should have at least two individuals with the expertise to administer the particular system;
6.11.3 All of the Trust's critical computer systems should have at least three individuals with the expertise to manage or administer such a system;
6.11.4 System managers will be responsible to the Senior Information Risk Owner for continued system security.

7 RISK MANAGEMENT

7.1 **Objective (International Standard ISO/IEC 27001:2013)**

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

7.2 Methodology (BS ISO/IEC 27001:2013 – 6.1.2, 8.2)

7.2.1 All systems will be subject to periodic security reviews by system managers. The depth of a review will be determined by the importance and size of the particular system.
7.2.2 Individual systems should be reviewed at least once every three years.
7.2.3 Reviews will include:
7.2.3.1 identification of assets of the system;
7.2.3.2 evaluation of potential threats;
7.2.3.3 assessment of likelihood of threats occurring;
7.2.3.4 identification of practical cost effective counter measures;
7.2.3.5 implementation programme for counter measures.
7.2.4 Systems are liable to independent reviews by internal and external auditors.

7.3 Reporting (BS ISO/IEC 27001:2013 – A.16.1.2)

Each system review will include a formal report to the Trust's management containing finding and recommendations

8 PERSONNEL SECURITY

8.1 Objective

To reduce the risks of human error, theft, fraud or misuse of facilities.

8.2 Employment (BS ISO/IEC 27001:2013 – A.7.1.2)

8.2.1 Terms and conditions of employment will:
8.2.1.1 • include the employee's responsibility for information security;
8.2.1.2 • require an employee to sign a confidentiality agreement.
8.2.2 Violations of this policy and associated procedures by employees shall be dealt with through a formal disciplinary process.
8.2.3 Job descriptions will include the appropriate security roles and responsibilities specified in this Policy.
8.2.4 Recruitment to specific roles managing IM&T systems will be subject to verification checks to include validating their technical capabilities, academic and professional qualifications, and taking up references.

8.3 User training (BS ISO/IEC 27001:2013 – A.7.2.2)

8.3.1 All employees and relevant third party users shall receive appropriate training and regular updates in the Trust's policies and procedures.
8.3.2 Authorised users of IM&T systems shall receive appropriate system training before authorisation is granted.

8.4 Monitoring security incidents and malfunctions (BS ISO/IEC 27001:2005 – A.13.1.2)

8.4.1 Security incidents shall be formally reported as soon as practicable after the incident is discovered.
8.4.2 Information system users shall note and report any:
8.4.2.1 Observed or suspected security weaknesses or threats;
8.4.2.2 Software malfunctions;

and these reports will be quantified and monitored.

9 EQUIPMENT SECURITY

9.1 Objective (International Standard ISO/IEC 27001:2013)

To protect IM&T equipment (to include all types of hardware and software) against loss or damage and avoid interruption to business activity.

9.2 Purchase of Equipment

9.2.1 All items of hardware and software purchased must comply with the Trusts minimum technical standards.

9.2.2 All IT equipment must be appropriately approved before purchase.

9.2.3 IT equipment purchased by an individual member of staff for business use (e.g. memory sticks) should be notified to the Head of Clinical Systems Development or her team.

9.3 Equipment siting and protection (BS ISO/IEC 27001:2013 – A.11.2.1)

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

9.3.2 Equipment should be sited to reduce risks from environmental threats, and from unauthorised access. Where equipment must be kept in public areas, it should be positioned to reduce the risk of unauthorised access or casual viewing.

9.3.3 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.

9.3.4 Smoking, drinking, eating and the use of mobile phones or other radio-frequency devices is not allowed in areas housing computer and network equipment and doors should be kept closed at all times. Warning signs to this effect must be prominently displayed at the entrance.

9.3.5 Appropriate measures must be taken to minimise the risk of theft of computing equipment. Consideration shall be given to measures such as secure anchoring of such equipment in public places and security coding.

9.4 Power supplies (BS ISO/IEC 27001:2013 – A.11.2.2)

9.4.1 The Trust has generator backup power to the mains electricity supply.

9.4.2 Critical computer equipment will be fitted with battery back-up, (using uninterruptible power supplies (UPS), to ensure it does not fail during switchovers between mains and generator. These UPS units must provide sufficient power to ensure the relevant system(s) can be shut down gracefully in the event of supply restoration/generator back-up not being available. Where a system is not manned continually, management software should be installed to allow the automatic shutdown of the system in the event of a power failure.

9.4.3 Critical computer sites will be fitted with emergency power off switches for use in a crisis. Such sites will have their own mains circuits not subject to power surges from other parts of the Trust.

9.5 Cable routing (BS ISO/IEC 27001:2013 – A.11.2.3)

9.5.1 All cabling (electricity or communications) between buildings will be via underground conduit not accessible to unauthorised people.
9.5.2 All cabling within buildings will be in conduits if surface mounted, otherwise within the framework of the building.
9.5.3 Suitable Cable Trays will be used for computer cables and these will be sited in accordance with the relevant standards in relation to electrical and heating services.

9.6 Equipment maintenance (BS ISO/IEC 27001:2013 – A.11.2.4)

9.6.1 All central processing equipment, including file servers, will be covered by third party maintenance agreements.
9.6.2 All personal computers, terminals and printers will be covered by maintenance agreements (where such provision is not in-house) 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 IT Department.
9.6.3 All such third parties will be required to sign confidentiality agreements.
9.6.4 Records of all faults/suspected faults will be maintained by the IT Department.

9.7 Remote diagnostic services (BS ISO/IEC 27001:2013 – A.15.1.1 & 15.1.2)

9.7.1 Suppliers of central systems/software expect to have dial up access to such systems on request to investigate/fix faults. The Trust will permit such access subject to it being initiated by the computer system and all activity monitored.
9.7.2 Each supplier requiring remote access will be required, before access is granted, to provide a written commitment to maintain confidentiality of data and information and only use qualified representatives.
9.7.3 Each request for dial up access will be authorised by approved computer services staff, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed/supplier ends his session.
9.7.4 Modem links will NOT be connected except in response to authenticated supplier request to prevent the possibility of unauthorised access.
9.7.5 Enhanced modem security incorporating strong authentication measures should be introduced as soon as practicable for additional security.

9.8 Security of data media

9.8.1 Hard disks on any machine and removable devices to backup/compress data may contain sensitive/confidential data. Removal off site of such disks/storage media 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 degaussed.

9.9 Security of equipment off premises (BS ISO/IEC 27001:2013 A.11.2.6)

9.9.1 Equipment and data will not be taken off site without formal signed approval of the appropriate line manager, other than to transport it from one of the Trust's sites to another.
9.9.2 Portable equipment should be provided with appropriate access protection, for example, passwords and/or encryption, and should not be left unattended in public places. Portable equipment is very vulnerable to theft, loss or unauthorised

access. Strong security measures should be introduced as soon as practicable, particularly if such equipment has network access capability.

9.9.3 Mobile devices must be properly updated with the latest anti-virus software where this is available.

9.9.4 To preserve the integrity of data, frequent synchronisations should be made with system computers. They should be maintained regularly, batteries kept charged to preserve their availability.

9.9.5 All portable equipment must be returned to IT Department for an asset verification and security check every three months.

9.9.6 SEE ALSO ACCEPTABLE USE OF TRUST INFORMATION ASSETS AND SYSTEMS AND 'USB, REMOVABLE MEDIA AND MEDIA DESTRUCTION POLICY'.

9.10 Mobile computing and teleworking (BS ISO/IEC 27001:2013 – A.6.1.1-2)

9.10.1 Any equipment used off site that processes the Trust's data must have prior signed approval of the appropriate line manager. Third party equipment must meet at least the physical and logical security controls implemented on the Trust's equipment.

9.10.2 The appropriate line manager must formally approve equipment provided for routine use off site. Such equipment may only access the Trust's networks or NHS*net*, and these only by remote access controls implemented by the IT Manager.

9.10.3 SEE ALSO 'REMOTE ACCESS and WORKING POLICY'.

9.11 Disposal of equipment (BS ISO/IEC 27001:2013 – A.8.3.2)

9.11.1 Computer hardware disposal can only be authorised by the IT Department. They should ensure that data storage devices are purged of sensitive data before disposal or securely destroyed. The procedures for disposal must be documented. All disposals must meet current National and EU Regulations.

10 Assets Inventory

10.1 Objectives (International Standard ISO/IEC 27001:2013)

10.1.1 To identify the location of the Trust's computer assets

10.1.2 To identify and authorise the use to which such assets are put

10.1.3 To manage capital charges on physical assets

10.2 Physical assets (BS ISO/IEC 27001:2013 – A.8.1.1)

An up to date register of acquisitions and disposals of physical information assets will be maintained. This will include the value, location, serial number and system manager primarily responsible for the maintenance of the asset. This register will normally be maintained by the IT Department.

10.3 7.3 Software

An up to date register of all proprietary software will be maintained to ensure that the Trust is aware of its assets and that licence conditions are followed. This register will normally be maintained by the IT Department.

10.4 7.4 System "ownership" (BS ISO/IEC 27001:2013 – A.8.1.2)

Each of the Trust's systems will be the responsibility of a specified system manager or Information Asset Owner whose responsibilities will include ensuring compliance with the Trust's Information Security Policy, ensuring the appropriate use of the equipment, troubleshooting and maintenance.

11 ACCESS CONTROL TO SECURE AREAS

11.1 Objective (International Standard ISO/IEC 27001:2013)

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

11.2 Physical security (BS ISO/IEC 27001:2013 – A.11.1.1)

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

11.2.2 The Trust's central computer suite will be a high security area housing its most important on site computers. An entry restriction and detection system will be incorporated to protect the suite.

11.2.3 Local network equipment/file servers and NHS*net* terminating equipment will always be located in secure areas and/or lockable cabinets.

11.3 Entry controls (BS ISO/IEC 27001:2013 – A.11.1.2)

11.3.1 Unrestricted access to the central computer facilities will be confined to designated staff, whose job function requires access to that particular area/equipment. The Technical Programmes Manager may give restricted access to other staff where a specific job function demands such access.

11.3.2 Authenticated representatives of third party support agencies will only be given access through specific authorisation from the Technical Programmes Manager.

12 SECURITY OF THIRD PARTY ACCESS

12.1 Objective (International Standard ISO/IEC 27001:2013)

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

12.2 Access control

12.2.1 No external agency (NHS or otherwise) 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.

12.2.2 External agencies will only be allowed access to their hardware/systems.

12.2.3 The Trust will control all external agencies access to its systems by enabling/disabling modem connections for each approved access requirement.

12.3 NHSnet requirements

12.3.1 Strong authentication procedures/technology must be introduced for ***all*** dial up connections to the Trust's computer systems where concurrent connection to the NHS*net* is possible.

12.3.2 Organisations should request that third parties providing remote support do so over NHS*net*. NHS Connecting for Health, Information Governance Team should be approached for advice prior to allowing access by third parties to an organisation's system.

12.4 Facilities management (FM) BS ISO/IEC 27001:2013 – A.5.1.2)

FM agencies should conform to both organisation and NHS Executive security requirements.

13 USER ACCESS CONTROL

13.1 Objective

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

13.2 Registering users (BS ISO/IEC 27001:2013 – A.9.2.1)

13.2.1 Formal procedures will be used to control access to systems. An authorised manager should countersign each application for access. Access to certain systems (NSTS) will require specific authorisation from the Caldicott Guardian.

13.2.2 Access privileges will be modified or removed, as appropriate, when an individual changes job or leaves.

13.2.3 For access to NPfIT Systems via smartcards, reference should be made to the Trust's RA Policy and procedures.

13.3 User password management (BS ISO/IEC 27001:2013 – A.9.4.3)

13.3.1 No individual will be given access to a live system unless properly trained and made aware of his or her security responsibilities.

13.3.2 Passwords must be at least six characters long. Users must keep their passwords secret and never disclose them to colleagues.

13.3.3 Passwords must be changed at least every 30 days. All new systems must include password ageing to force users to change their password.

13.3.4 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.

14 SECURITY INCIDENT MANAGEMENT

14.1 Objective (BS ISO 27001:2013 A16)

To detect, investigate and resolve any suspected/actual computer security breach.

14.2 Security incidents (BS ISO 27001:2013 – A.16.1.2 & A.16.1.3)

14.2.1 A security incident is an event that may result in:

- 14.2.1.1 degraded system integrity;
- 14.2.1.2 loss of system availability;
- 14.2.1.3 disclosure of confidential information;
- 14.2.1.4 disruption of activity;
- 14.2.1.5 financial loss;
- 14.2.1.6 legal action;
- 14.2.1.7 unauthorised access to applications

14.2.2 The Information Security Manager will report incidents to the NHS Executive's Security and Data Protection Programme.

14.2.3 All security incidents that may have an impact on NHS*net* will be reported immediately, by the Information Security Manager, to the appropriate Local NHSnet Security Manager.

14.2.4 Security breaches may result in disciplinary action.

14.3 Individual's responsibilities (BS ISO/IEC 27001:2013 – A.16.1.3)

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

14.3.2 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.

14.4 Logging security incidents

All actual security incidents will be formally logged, categorised by severity and action/resolution recorded by the relevant system manger and reported to the Information Security Manager and, where appropriate, to the Caldicott Guardian.

15 HOUSEKEEPING

15.1 Objective

To maintain the integrity and availability of computer assets.

15.2 Data backup (BS ISO/IEC 27001:2013 – A.12.3.1)

15.2.1 All central systems will have daily backup regimes formalised in the appropriate job run manual. Such backups will have a minimum of a 5 day cycle before media is overwritten. Secure storage will be used for 4 of the 5 backups with only the next one to be used being on site. Such storage should be geographically separate from the system location to protect against building loss.

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

15.2.3 All PC users, where central storage of data is not provided, are advised to backup their data regularly with a minimum 3 day cycle (preferably 5) before media is overwritten. Procedures have already been issued to all users.

15.2.4 The Trust encourages the use of the network for storage of all data which is backed up daily by the IT Department.

15.3 Incident reporting

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

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

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

15.4 Controlled stationery

(e.g. payment stationery, drug ordering, prescriptions etc.).

15.4.1 Formal procedures have been established to control and account for the use of such stationery.

15.4.2 Each should include some form of unique identifier to assist control management. These procedures should be maintained within each relevant department.

15.5 Security of Media in Transit (BS ISO/IEC 27001:2013 – A.8.3.3)

15.5.1 Reliable transport or couriers should be used, and a procedure to check the identity of couriers in the event of loss or damage of media or equipment should be implemented.

15.5.2 Packaging should be sufficient to protect the contents from any physical damage likely to arise in accordance with the manufacturer's specifications. Regard should be given to any adverse environmental conditions that may occur during transit.

15.5.3 Special controls should be adopted, where necessary, to protect patient-identifiable and other sensitive information from unauthorised disclosure or modification, such as:

15.5.3.1 Use of Locked Containers

15.5.3.2 Delivery by Hand

15.5.3.3 Tamper-evident packaging

16 DATA VALIDATION

16.1 Objective

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

16.2 At data input (BS ISO/IEC 27001:2013 – 7.5.3)

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

16.2.2 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.

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

16.2.4 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.

16.2.5 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).

16.3 Internal validation (BS ISO/IEC 27001:2013 –9.2)

16.3.1 All computer systems should incorporate internal validation processes and audit trails to detect and record problems with processing and data integrity.

17 SOFTWARE PROTECTION

17.1 Objective (ISO 27001:2013 – 12.5.1)

To comply with the law on licensed products and minimise risk of malicious software.

17.2 Licensed software

17.2.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action and civil and criminal prosecution. Each user should ensure that a copy of each licence for commercial software is held by the IT Department.

17.3 Organisation's software standards

17.3.1 The Trust will only permit approved software to be installed on its PCs. The IT Department will approve, and install, all software.

17.3.2 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 must be phased out as soon as practicable.

17.3.3 Where the Trust recognises the need for specific specialised PC products, such products should be registered with the IT Department and be fully licensed.

17.4 Malicious software (BS ISO/IEC 27001:2013 – A.12.2.1)

17.4.1 The Trust seeks to minimise the risks of malicious software through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas.

17.4.2 Users should report any viruses detected/suspected on their machines immediately to the IT Department via the Helpdesk to be recorded on the incident log.

17.4.3 All occurrences of viruses must be dealt with as a high priority to ensure that the spread of the virus is kept to an absolute minimum.

17.4.4 No newly acquired disks, magnetic media, or CDs, from whatever source, are to be loaded unless they have previously been virus checked by a locally installed virus-checking package.

17.4.5 Email attachments must be checked before they are opened.

18 BUSINESS CONTINUITY PLANNING

18.1 Objective

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

18.2 Need for effective plans (BS ISO/IEC 27001:2013 – A.17.1.1)

18.2.1 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 business continuity plans.

18.2.2 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.

18.2.3 The Trust requires tried and tested business continuity plans for its computing facilities to be maintained.

18.3 Planning process (BS ISO/IEC 27001:2013 – A.17.1.1)

18.3.1 The main elements of this process will include:

- 18.3.1.1 identification of critical computer systems
- 18.3.1.2 identification and prioritisation of key users/user areas
- 18.3.1.3 agreement with users to identify disaster scenarios and what levels of business continuity are required
- 18.3.1.4 identification of areas of greatest vulnerability based on risk assessment
- 18.3.1.5 mitigation of risks by developing resilience

18.3.1.6 developing, documenting and testing business continuity plans identifying tasks, agreeing responsibilities and defining priorities

18.4 Planning framework (BS ISO/IEC 27001:2013 – A.17.1.2)

18.4.1 Business continuity plans cater for different levels of incident including:
- 18.4.1.1 loss of key user area within a building;
- 18.4.1.2 loss of a key building;
- 18.4.1.3 loss of key part of computer network;
- 18.4.1.4 loss of processing power.

18.4.2 Business continuity plans always include:
- 18.4.2.1 emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting business continuity personnel);
- 18.4.2.2 fallback procedures describing the actions to be taken to provide contingency devices defined in the business continuity plan;
- 18.4.2.3 resumption procedures describing the actions to be taken to return to full normal service;
- 18.4.2.4 testing procedures describing how the business continuity plan will be tested.

18.4.3 Business continuity plans are kept in the IT Department.

18.5 Objective

18.5.1 Appropriate cryptographic controls shall be used to ensure the integrity and confidentiality of the communication, processing and storage of sensitive information in accordance with the Trust policy.

18.5.2 Emphasis is placed upon external communications, but the provisions also apply equally to internal communications where they may be a risk of compromising confidentiality.

18.6 Key Management (BS ISO/IEC 27001:2013 – A.10.1.2)

18.6.1 Adequate measures shall be taken to minimise the risk of loss or compromise of cryptographic keys, which shall include:
- 18.6.1.1 Defined activation and deactivation dates so that keys can only be used for a limited period.
- 18.6.1.2 Logging and auditing of key management related activities (e.g. creation, destruction and archiving)
- 18.6.1.3 Procedures for the revocation of keys (e.g. on staff termination or key compromisation)
- 18.6.1.4 Procedures shall be in place for the production of cryptographic keys in the event of an authorised person making a written request in accordance with the Regulation of Investigatory Powers Act 2000.

19 EQUALITY IMPACT ASSESSMENT STATEMENT

19.1 All public bodies have a statutory duty under the Race Relation (Amendment) Act 2000 to “set out arrangements to assess and consult on how their policies and functions impact on race equality.” This obligation has been increased to include equality and human rights with regard to disability, age and gender.

19.2 The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. This strategy was found to be compliant with this philosophy.

19.3 Equality Impact Assessments will also ensure discrimination does not occur on the grounds of Religion/Belief or Sexual Orientation in line with the protected characteristics covered by the existing public duties.

19.4 Refer to appendix 1.

20 Equality Impact Assessment Tool – Appendix 1

		Yes/No	Comments
1	Does the policy/guidance affect one group less or more favourably than another on the basis of:	No	
	▪ Race	No	
	▪ Disability	No	
	▪ Gender	No	
	▪ Religion or belief	No	
	▪ Sexual orientation including lesbian, gay and bisexual people	No	
	▪ Age	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	N/A	
4	Is the impact of the policy/guidance likely to be negative?	No	
5	If so can the impact be avoided?	N/A	
6	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

21 MONITORING & REVIEW

What will be monitored	How/Method/ Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions	Implementation of any required change
Policy review	Every 2 years	Information Governance Manager/ Technical Programmes Manager	Information Governance Committee	Information Governance Committee	Senior Managers
Information Security incidents	Regular agenda item Information Governance Steering Group	Information Governance Manager	Information Governance Committee	Information Governance Committee	Relevant Senior Managers
Information Asset Register	Annual review	Technical Programmes Manager	Information Governance Committee	Information Governance Committee	Relevant Senior Managers
Information Security risks	Regular agenda item Information Governance Steering Group	Information Governance Manager	Information Governance Committee	Information Governance Committee	Relevant Senior Managers
Access control (Secure Areas)	Annual Review	Technical Programmes Manager	Information Governance Committee	Information Governance Committee	Health Applications Implementation Manager Delivery
Access control (systems)	Quarterly	System Managers	Information Governance Committee	Information Governance Committee	Relevant Senior Managers
Business Continuity Planning	Annual Review	Technical Programmes Manager	Information Governance Committee	Information Governance Committee	Associate Director for Service Development

22 ANNEX A – BS ISO/IEC 27001:2013

BS ISO/IEC 27001:2013 is the British Standard on Information Security Management developed by the British Standards Institute and the Department of Trade and Industry with the cooperation of various public and private sector organisations, including healthcare. There are two parts to the application of the standard:
Part 1 is a *Code of Practice for information security management* and provides a comprehensive set of security objectives and control requirements for those organisations seeking to demonstrate compliance with the British Standard.
Part 2 is a specification for information security management, suitable for certification of an organisation's information security management system.

They provide a set of key controls considered necessary to comply with the standard and detailed guidance to assist in the implementation of information security. However not all of the controls described are relevant to every situation, and do not take account of local environmental factors or technological constraints. The objective is “to provide organisations with a common basis for providing information security and to enable information to be shared between organisations”, which is particularly significant with the increased electronic exchange of information.
The NHS, in *Building the Information Core: Implementing the NHS Plan*, has adopted this standard..
Organisations seeking to be certified as complying to this British Standard will need to undertake a risk assessment to identify the control objectives and controls to be implemented, applicable to the Trusts own needs. These are recorded in a Statement of Applicability, which would have to be freely available to internal managers, personnel and auditors as well as appropriate external organisations (e.g. certifiers).
Certification does not imply achievement of specific levels of information security for its activities, products or services and compliance with this standard does not of itself confer immunity from legal obligations.

23 ANNEX B - ABBREVIATIONS

CCTA	Central Computer and Telecommunications Agency
CRAMM	CCTA Risk Analysis and Management Method
FM	Facilities management
IM&T	Information Management and Technology
IT	Information Technology
NHS	National Health Service
NI	National Insurance
PC	Personal computer
PDA	Personal digital assistant (handheld computer)
UPS	Uninterruptible power supply
UK	United Kingdom
WAP	Wireless application protocol (a means of viewing data from the internet on a mobile phone)

24 ANNEX C - GLOSSARY

For the purposes of this policy the following definitions apply:

access control	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner
accountability	The property that will enable the originator of any action to be identified (whether the originator is a human being or a system)
application manager	Nominated person responsible for the operational management and development of software for a specific system
asset owner	Individual or organisation having responsibility for specified information asset(s) and for the maintenance of appropriate security measures
audit trail	Data collected and potentially used to facilitate any reconstruction of events within the system
authentication	Corroboration of the origin and correctness of any part of the system.
authorisation	The granting of rights, which includes the granting of access based on access rights
availability	Information is delivered to the right person, when it is needed
confidentiality	Data access is confined to those with specified authority to view the data
CRAMM	The CCTA Risk Analysis and Management Method
data controller	Data controller means a person who (alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed and the data are in the form in which they have been or are intended to be processed or recorded with that intention or as part of a relevant filing system or is part of an accessible record and processing means obtaining, recording or holding the information or data, including organisation, retrieval, disclosure, blocking, erasure or destruction. [Data Protection Act (1998)]
degauss	To remove unwanted magnetic fields and effects from magnetic disks, tape or read/write heads
denial of service	The prevention of authorised access to resources or the delaying of time critical operations
health professional	Any of the following: • a registered medical practitioner • a registered dentist • a registered optician

	• a registered pharmaceutical chemist • a registered nurse, midwife or health visitor • a registered osteopath • a registered chiropractor • any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends • a clinical psychologist, child psychotherapist or speech therapist • a music therapist employed by a health service body, or • a clinical and biomedical scientist employed by such a body as head of a department.
health record	This is any record which consists of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual
Impact	The embarrassment, harm, and financial loss, legal or other damage which could occur in consequence of a particular security breach
Information security	Protection of information for: • confidentiality • integrity • availability
Integrity	All system assets are operating correctly according to specification and in the way that the current user believes them to be operating
NHS Organisations	All organisations providing health care services, including health authorities, special health authorities, trusts, general medical and dental practices
password	Confidential authentication information composed of a string of characters
personal data	Data consisting of data which relate to a living individual who can be identified from that data (or from that and other information in the possession of, or likely to come in the possession of, the Data Controller), including any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual [Data Protection Act (1998)]
personally-identifiable information	Key data items which may be used to identify a person include: • National identifier: e.g. NHS Number, or NI Number • Local identifier, e.g. hospital or System ID Number • Name • Address • Postcode • Date of Birth • Other Dates, e.g. death, diagnosis • Sex • Ethnic Group • Occupation [*Caldicott Committee: Report on the review of patient-identifiable information - December 1997*]

Portable Equipment	Includes laptop and notebook computers, PDAs, and third generation, WAP-enabled mobile telephones
recovery	Restoration of a system to its desired date following a failure in the operation of the system
risk	The likelihood of occurrence of a particular threat, with the degree of vulnerability to that threat and the potential consequence of the impact if the threat occurs
risk assessment	Comprehensive concept for defining and assessing the potential impact of threats to, and vulnerabilities of, computer system assets and capabilities, and for supplying management with information suitable for a (risk management) decision in order to optimise investment in security counter-measures
security audit	A review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures
security breach	Any event that has, or could have, resulted in loss or damage to NHS assets, or an action that is in breach of NHS security procedures
security policy	A statement of the set of rules, measures and procedures that determine the physical, procedural and logical security controls imposed on the management, distribution and protection of assets
sensitive personal data	This is data as to the Data Subject's: • racial or ethnic origin • political opinions or religious beliefs • trade union membership • physical or mental health or condition • sexual life • criminal offences, proceedings or convictions [*Data Protection Act (1998)*]
sensitivity	A measure of importance assigned to information to denote its confidentiality
special privilege	Any feature or facility of a multi-user system that enables a user to override system or application controls
system manager	Nominated IM&T person responsible for the hardware and operating system and database management for a specific system
threat	An action or event that might prejudice security
Vulnerability	A security weakness

25 Appendix D - KEY POINTS FOR USERS

Information Security

25.1 The aim of an information security policy is to ensure that information:

- 25.1.1 Stays private, with only authorised people able to view it (confidentiality);
- 25.1.2 Is not tampered with (integrity);
- 25.1.3 Is available when required (availability).

25.2 All members of staff, and any other authorised users, are responsible for ensuring that no breaches of security result from their actions. (A *breach* is any event that has, or could have, resulted in loss or damage to NHS assets; or an action that is in breach of NHS security procedures.) To achieve this you must follow these rules:

- 25.2.1 Keep computer screens clear while unattended so as to protect the network from unauthorised access. Log off when no longer working at the desktop or, if planning to return to the terminal after a short time, either lock the workstation or activate the password-controlled screensaver.
- 25.2.2 Be responsible for the accuracy and currency of data you record on systems;
- 25.2.3 Store confidential information on the network, not on your local PC;
- 25.2.4 Back up data to the network server at regular intervals throughout the working day;
- 25.2.5 Ensure that any data on local hard drives (e.g. on laptops) is uploaded to the server.
- 25.2.6 Store removable media holding confidential data in a secure location;
- 25.2.7 Report to the Information Security Manager any security incidents, weaknesses or threats or software malfunctions;
- 25.2.8 Be aware of the Computer Misuse Act 1990[1]. Do not intentionally gain access to a computer program or data knowing that you are not entitled to do so; and do not use unauthorised access to commit further offences such as altering, erasing, copying or moving the program or data;
- 25.2.9 Do not use the computer system to snoop or pry into the affairs of the other users by unnecessarily reviewing their files or emails.
- 25.2.10 Do not use your own IT equipment (e.g. laptops, memory sticks) without explicit permission from the Information Security Manager;
- 25.2.11 Follow the Trust's guidance on use of IT equipment and data outside Trust premises.
  (See policies on USB,Removable Media and Media Destruction and Remote Access and Working.)
- 25.2.12 Remember that you are responsible for safeguarding your password(s) and are
- 25.2.13 responsible for all transactions, email or internet browsing using your password. Do not print, store online, or give your password to others.
- 25.2.14 Do not allow anyone else to work under your logon.
- 25.2.15 Do not access the Trust's computer systems with another user's password or account.
- 25.2.16 Use commercial software only if it has been approved, installed and licensed by the IT Department.
- 25.2.17 Do everything you can to prevent the introduction of malicious software on the Trust's information systems.

[1] For a full description of the Computer Misuse Act, see "NHS Information Governance: Guidance on Legal and Professional Obligations", DH, Sept 2007, section 1.12

25.2.18 Immediately report to the IT Help Desk any viruses that you have detected, or suspect, on your machine.

25.2.19 Do not use any removable media (such as disks or memory sticks), even if newly acquired, unless they have first been checked by a locally installed virus-checking package.

25.2.20 Do not open email attachments without first checking them for viruses.

For a full guide to this subject, see the Information Security Policy and the Network Security Policy.

END OF DOCUMENT