Frimley Health NHS
NHS Foundation Trust

Information Security Policy

Key Points

- Set out business processes that protect confidentiality, integrity and availability of both manual and electronic information.
- Minimise unauthorised disclosure, modification, removal or destruction of the Trust's information assets, and disruption to NHS business activities will be minimised.
- The Trust's obligation to comply with legislation and guidance issued by the Department of Health.
- All staff are made aware that any breaches of confidentiality and Information Security should be reported and investigated.
- All staff have a duty to ensure that they do not put the Trust's information assets at risk and that they protect the confidentiality of personal and sensitive information.
- All records or documents will be classified according to their sensitivity using the guidance from the Department of Health
- All IT equipment will be disposed of via IT Service Desk
- All breaches of information must be reported immediately as per the procedure and a reassessment of risks should be made.
- The consequence of a confidentiality and/or security breach can lead to disciplinary action and/or criminal prosecution.
- The Trust has identified Safe Haven areas for the transmission of confidential and sensitive information.

Version:	1.2
Role of Policy Lead(s):	Head of Information Governance
Role of Executive Lead:	Director of Finance
Date Approved by Executive Lead:	3rd October 2016
Name of Responsible Committee:	Information Governance Committee
Date Approved by Professional Approving Group:	1st October 2018
Date Approved by Policy Review Group:	March 2017
Date Ratified by Hospital Executive Board:	March 2017
Date Issued:	March 2019
Review Date:	March 2020
Target Audience:	All Trust staff
Key Words & Phrases:	Information, Security, protection, network, electronic, paper

Version Control Sheet

Version	Date	Policy Lead(s)	Status	Comment
0.1	26/09/2016	Nicola Gould	Draft	Revised policy following acquisition
1.0	28/03/17	Policy Officer	Final	Ratified at HEB March 2017
1.1	27/07/18	Information Governance Administrator	Interim	Update of Definitions
1.2	19/09/2018	Head of Information Governance	Interim	Update for GDPR and adding in Cyber Security

Document Location

Document Type	Location
Electronic	Policy Hub (Trust-wide)

Related Documents

Document Type	Document Name
Policy	Data Protection and Confidentiality Policy
Policy	Remote Access Policy
Policy	Non-Clinical Records Management Policy
Policy	Email Policy
Policy	Internet Policy
Policy	Risk Management Policy
Policy	Incident Reporting Policy
Policy	Caldicott Principles

Contents

1. INTRODUCTION

1.1 Information, whether in paper or digital form, is the lifeblood of Frimley Health NHS Foundation Trust because of its critical importance to NHS patient care and other related business processes.

1.2 High quality information underpins the delivery of high quality evidence-based healthcare and many other key service deliverables. Information has the greatest value when it is accurate, up to date and is accessible where and when it is needed.

1.3 An effective information security management regime ensures information is properly protected and is reliably available. Without effective security, the Trust's information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised parties.

1.4 Effective information security management is underpinned by robust information risk management processes. These processes require the Trust to have a robust information risk management structure in place that reduces risks and threats to information whilst retaining its security, availability and accessibility.

1.5 Frimley Health NHS Foundation Trust is committed to the provision of a service that is fair, accessible and meets the needs of all individuals.

2. SCOPE

2.1 This policy applies to all information, information/communications systems, networks, applications, locations and users, including information held on all types of removal media, e.g., USB Sticks, memory cards owned by the Trust.

2.2 This policy also applies to:

- all Trust staff engaged in work for the Trust at any location, on any computer or internet connection;
- any other use by Trust staff which identifies the person as a Trust member of staff or which could bring the Trust into disrepute on any computer or internet connection;
- any other person working for the Trust, persons engaged on Trust business or persons using Trust equipment and networks;
- all usage by any person granted access to the Trust network;
- any other person who may process information on behalf of the Trust.

2.3 All members of staff identified in 2.2 are required to comply fully with this policy.

3. DEFINITIONS

3.1 **Confidentiality of information -** Person-identifiable, sensitive or otherwise valuable information will be protected against unauthorised access and disclosure.

3.2 **Information Assets -** Any information that is stored physically or electronically, transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed.

3.3 **Physical, logical, environment and communications security -** Controls to prevent unauthorised access, damage and interference to Information Management & Technology (IM&T) services and clinical records.

3.4 **Infrastructure -** Computers, systems, networks, cabling and other devices which make up the estate of information management in the Trust.

3.5 **Forensic Readiness -** The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.

3.6 **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.

3.7 **Information Security Event –** Indicates that the security of an information system, service, or network may have been breached or compromised, i.e., the safeguards put in place may have failed.

3.8 **Information Security Incident –** Is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.

3.9 **Encryption –** The conversion of electronic data into another form which cannot be easily seen by anyone except authorised parties.

3.10 **Threat –** Is a potential event which, when it actually takes place, can result in an unwanted incident.

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

3.12 **Risk Analysis –** Uses information to identify possible sources of risk.

3.13 **Risk Evaluation -** Compares the estimated risk with a set of risk criteria to determine how significant the risk is.

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

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

3.16 **Safe Haven –** A safe haven is a location which is set up to receive and manage confidential information appropriately. It may be a post room, reception area or fax machine or anywhere messages may be taken and held before being passed onto the appropriate recipient.

3.17 **Information Governance Statement of Compliance -** The Information Governance Statement of Compliance (IG SoC) is the process by which organisations enter into an agreement with NHS Digital for access to the NHS National Network (N3).

3.18 **Business Continuity Plan –** Is defined as the "capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident." (ISO 22300).

3.19 **Disaster Recovery Plan –** Describes how the Trust restores information systems affected by a disaster. It ensures the IM&T Department prepares for disaster recovery, meets recovery needs agreed in Business Continuity plans, prioritises and co-ordinates recovery tasks in the event of multiple losses, keeps the organisation informed of the occurrence, impact and progress to recover from a disaster.

3.20 **Third Party -** A third party is any person or organisation that is independent or not employed by the Trust.

3.21 **N3 –** N3 is the Legacy national broadband network for the NHS. It is a Wide Area IP Network (WAN), connecting many different sites across the NHS within England & Scotland. The N3 network is now being phased out and replaced by HSCN (Health and Social Care Network)

3.22 **Serious Untoward Incident -** A Serious Untoward Incident is "an incident or series of incidents (in which one or more patients are involved) which are likely to produce significant legal, media or other interest or give rise to large scale public concern and which, if not properly managed, may result in significant loss of the Trust's reputation and/or assets".

3.23 **Common Law –** A law which is determined by decisions made by the courts and can therefore change over time. A law set by precedents.

3.24 **Senior Information Risk Owner (SIRO)** - is an Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy.

The SIRO is accountable and responsible for information risk across the organisation. They ensure that everyone is aware of their personal responsibility to exercise good judgment, and to safeguard and share information appropriately.

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

3.26 **BC/DR** – Business Continuity/Disaster Recovery

3.27 **Browser** - A software program that allows a user to interact with resources on the internet. Common browser programs include Internet Explorer, Mozilla Firefox and Google Chrome.

3.28 **Business critical** - An element of a process without which the remainder of the process cannot function.

3.29 **Control** - Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature.

3.30 **Conversion/migration** - Process of changing records from one medium to another or from one format to another.

3.31 **Cyber Attack** - A cyber attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks.

3.32 **Cyber Incident** - Any malicious act or suspicious event that: Compromises, or was a attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

3.33 **Cyber Security** – Cyber security, computer security or IT security is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

3.34 **IM & T** - Information Management and Technology.

3.35 **Information** - A collection of data with which the user can gain knowledge.

3.36 **Information Asset** - Anything that has value to the Trust.

3.37 **Information processing facilities** - Any information processing system, service or infrastructure, or the physical locations housing them.

3.38 **Information Security Incident** - A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

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

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

3.41 **Internet** - A network of computers linked worldwide to allow people to view, download and upload data. Referred to as ‘The Web’.

3.42 **ISO 17799** - International Standard – Code of Practice for information security management.

3.43 **Preservation** - Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time.

3.44 **Residual risk** - The risk remaining after risk treatment.

3.45 **Risk acceptance** -The decision to accept a risk.

3.46 **Risk treatment** - Process of selection and implementation of measures to modify risk.

3.47 **Threat** - A potential cause of an unwanted incident which may result in harm to a system or organisation.

3.48 **UPS** - Uninterruptible power supply

3.49 **Vulnerability -** A weakness of an asset or group of assets that can be exploited by one or more threats.

4. PURPOSE

4.1 The purpose of this Information Security Policy is to protect to a consistently high standard, all information assets, including manual and electronic records, both patient and other Trust corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

4.2 Adherence of this policy will prevent the unauthorised disclosure, modification, removal or destruction of NHS information assets, and disruption to NHS business activities.

4.3 The Trust's IM&T and Communications systems are for business purposes and the use of these systems are at all times subject to this policy and other named Trust policies/procedures.

4.4 The Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets within the Trust. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in:

- **Confidentiality** – data access is confined to those with specified authority to view the data on a need to know basis;
- **Integrity** – all system assets are processed correctly according to specification and in the way the current user believes them to be operating;
- **Availability** – information is delivered to the right person when it is needed.

4.5 The adoption of this policy will also provide Information Security Assurance for the purpose of the Data Security and Protection Toolkit.

5. THE POLICY

5.1 Policy Overview

5.1.1 Ensure that confidentiality, integrity and availability of all systems are maintained at all times.

5.1.2 Protect, to a consistently high standard, all information assets, including manual and electronic records, both patient and other Trust corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

5.1.3 Prevent unauthorised disclosure, modification, removal or destruction of NHS information assets, and disruption to NHS business activities.

5.1.5 Ensure legal obligations to maintain security and confidentiality under the Data Protection Act (2018), Human Rights Act (1998), Copyright, Designs and Patents Act (1988), Computer Misuse Act (1990) and the Freedom of Information Act (2000).

5.1.6 Ensure compliance with The Common Law Duty of Confidentiality which prohibits use or disclosure of personal information which has been given in confidence.

5.1.7 All staff must adhere to the seven Caldicott principles (Caldicott Report 2013).

5.1.8 All staff must also abide by the Department of Health Information guidance.

5.1.9 All staff are made aware of their Information Security responsibilities.

5.1.10 The Trust will have in place an appropriate information security management structure with clear reporting lines.

5.1.11 The Trust will identify IT Information Asset Owners and ensure that an inventory of IT assets is maintained and regularly updated.

5.1.12 The Trust will detect, investigate and resolve any suspected or actual computer breach.

5.1.13 The Trust will protect its computer and related equipment against loss or damage and avoid interruption to business activity.

5.1.14 All staff have a duty to ensure that they do not put the Trust's information assets at risk and that they protect the confidentiality and security of personal and other sensitive information. They must follow correct procedure at all times. Failure to do so could result in disciplinary action.

5.1.15 All breaches of information security, actual or suspected, shall be recorded, reported and investigated.

5.1.16 In common with other Serious Untoward Incidents (SUI), all personal data SUI's incidents relating to a breach of security, which then places the Trust's personal data at risk, must be reported to NHS Digital, the Department of Health and the Information Commissioners Office. (See 5.4.5 for further information on SUI's).

5.2 Information Risk

5.2.1 Information risk is inherent in all administrative and business activities which will be managed in a structured way through the Trust's current risk management framework.

5.2.2 Effective information security management is based upon the core principle of risk assessment and management. This requires the identification and quantification of information security risks in terms of their perceived severity of impact and the likelihood of occurrence.

5.2.3 The risk assessment management structure and processes identify how information-related risks are controlled.

5.2.4 Once identified, information security risks will be managed on a formal basis through the Information Governance (IG) Risk register and the action plans to mitigate the identified risk will be monitored by the Information Governance Committee and the Head of Information Governance. Risks will be recorded within a Trust risk register

and action plans will be developed to demonstrate the Trust's effective management of its information assets risks.

5.2.5 Where significant risks are identified, e.g., high or extremely high, these will be considered at Corporate Governance group for inclusion in the Corporate Risk Register.

5.2.6 The Trust's IG Risk register and all associated actions will be reviewed at regular intervals until no further action could be taken and the decision is taken to accept the risk.

5.2.7 The Trust's SIRO, Head of Information Governance, IAO's and IAA's will work in conjunction with the Risk Management Team to manage the Trust information security risks within the Trust's current risk management structure and arrangements.

5.3 Information Assets

5.3.1 The Trust's information assets will come in many different forms. Below is an example of the Trust's information assets:

Personal Information	**Software**
Patient records – manual/electronic Staff /Contractors records Clinical Audit Data Research Data Management / Performance Data Trust Membership records	Clinical Systems software Microsoft Office software Applications software System Software Development and maintenance tools
System / Process Documentation	**Hardware**
System information / Support documentation Information databases Back-up tapes / information Data files / Archive data / information Audit data	PC's/Computers Laptop IT Servers CDs / DVDs, USB sticks Printers, Scanners
Corporate Information	**Miscellaneous**
Meeting Minutes / Papers Financial information Trust Policies / Procedures / Guidance Presentations Trust Reports / Returns Operational Procedures / Manuals Contracts / Service Level Agreements	Staff skills / Experience / Knowledge

5.3.2 The Trust's Information Asset list will be managed and maintained by the Head of Information Governance in liaison with the Trust's IAO's.

5.3.3 The list will be grouped in a logical order, e.g., as per the example table at 5.3.1.

5.3.4 Given the constraints of time and resources, priority will be given to information assets that (a) contain personal information about patients or staff and/or (b) are

essential to the support of Trust operations, e.g., financial systems, infrastructure documentation.

5.3.5 All information received, and recorded by the Trust will have:

- an Owner - i.e., the person that is the business/clinical main user of the information, or the person that acquired the information from a third party;
- a Custodian – i.e., the person(s) that processes the information on behalf of the owner according to protocols defined by the owner;
- a User – i.e., the person using the information in accordance with legislation and regulation to perform their job functions.

5.3.6 These roles need to be identified when the Information Asset is entered onto the Trust's Information Asset Register.

5.3.7 Threats to NHS data shall be appropriately identified and based upon robust risk assessment and management arrangements, and shall be managed and regularly reviewed to ensure:

- protection against unauthorised disclosure;
- integrity and evidential value of information is maintained;
- information is available to authorised personnel as and when it is required.

5.4 Information Security Incident Management

5.4.1 All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

5.4.2 All Trust incidents must be reported using the Trust's incident reporting procedures and managed in line with the Trust's Incident Reporting Policy. All incidents must be reported as soon as they are identified.

5.4.3 Where there is an information security breach or event this will be managed by the Head of Information Governance and reported to the Trust's SIRO.

5.4.4 The Information Governance Committee will regularly review reported information security incidents and where applicable approve changes to Trust policies and procedures to reduce the risk of the information security incident reoccurring.

5.4.5 Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have a significant impact on an individual should be considered as serious, and could be reported as a Serious Untoward Incident. This applies irrespective of the media involved and includes both the loss of electronic media and paper records.

5.4.6 Where an information security breach is classified as an SUI this will be reported to the appropriate bodies, e.g., Monitor, Information Commissioner, Department of Health.

5.5 Cyber Security Incident Management

5.5.1 All staff are responsible for ensuring that no actual or potential Cyber Security breaches occur as a result of their actions.

5.5.2 All Trust Cyber Security incidents must be reported using the Trust's incident reporting procedures and managed in line with the Trust's Cyber Security Incident Response Plan. All incidents must be reported as soon as they are identified.

5.2.3 All staff must give their full support to any investigation carried out in response to the Cyber Security incident as important lessons may be learnt to reduce the risk of the type of incident occurring again.

5.2.4 Where there is a Cyber Security breach or event this will be managed by the Cyber Security Specialist and reported to the Trust's SIRO along with the CIO of IM&T.

5.2.5 All urgent Cyber Security incidents where significant loss of data, system availability, or control of systems is identified will be reported to NHS Digital within 72 hours of the incident being discovered.

5.2.6 An assessment of all Cyber Security breaches will be carried out post breach and follow-on actions may be required to be undertaken, this may include, update or change the incident response process, update or change the IT System configurations, or change the procedures, policies, standards or guidelines or introduce new ones to reduce the risk of that type of incident re-occurring.

5.6 Safe Haven

5.6.1 The Trust has identified a list of Safe Haven Areas which is maintained by the Information Governance Department.

5.6.2 The Trust has developed safe haven procedures for all methods of transferring confidential information, which staff must follow:

- post
- electronic / email
- transporting
- faxing
- bulk transfer

5.6.3 Where staff need to use an external courier, the Trust approved courier service must be used.

5.6.4 The faxing of confidential / patient information is not a secure method of transferring information. Before faxing confidential information staff should consider alternative methods for transferring information, e.g., email, post, removable media.

5.6.5 A fax cover sheet must ALWAYS be used when transmitting personal confidential information outside the Trust.

5.6.6 Any fax received in error must be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission.

5.6.7 Unsolicited or unexpected faxes should be treated with care until the sender has been identified.

5.6.8 All bulk transfers of 50 or more records should be communicated to the Information Governance Team with an explanation as why this transfer needs to occur and by which means it is being sent.

5.6.9 When transporting patient medical records, they should be properly sealed in an envelope or in the custody of the staff accompanying the patient.

5.7 Verbal Communication

5.7.1 The Trust has a legal obligation to ensure that all personal data being processed is kept secure (Data Protection Act principle 6).

5.7.2 The Trust's Data Protection and Confidentiality Policy states staff must ensure when holding confidential conversations these are not undertaken in a public area, or where a member of staff who does not need access to the confidential information can overhear the conversation.

5.7.3 Staff should also take extra care on the positioning of answer phones where messages containing confidential information can be left.

5.7.4 The identity of persons requesting and receiving sensitive or confidential information over the telephone must be verified, and they must be authorised to receive it.

5.7.5 All parties are to be notified in advance whenever telephone conversations are to be recorded.

5.8 Clear Desk Policy

5.8.1 The Trust must ensure that all confidential information is not left unattended and is removed to a secure location, e.g. locked filing cabinets and the codes of the cupboard are regularly changed to ensure staff who no longer have a need to access the records are not able to do so.

5.9 Sharing Confidential Information

5.9.1 Where there is a need for staff to share patient information with another NHS organisation, staff must ensure that the sharing of the information complies with both the Data Protection Act 2018 and the Common Law Duty of Confidentiality.

5.9.2 Sharing of confidential information must comply with the framework set out in the appropriate Information Sharing Protocols that the Trust has signed up to as well as Trust policies/procedures, e.g., information sharing protocols.

5.10 Access Control

5.10.1 The Trust will establish robust access controls to both its network and all IT systems. Access control will incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs and will be role based. Access controls will be issued on a strictly need to know basis and in accordance with legislation and regulation.

5.10.2 Access to the Trust's Network is documented in the Trust's Network Access procedure. Only staff who have successfully completed the Trust's PC Induction will be provided with access to the Trust's network.

5.10.3 Management of user accounts is detailed in the Trust's Network Access procedure, including the removal of user accounts.

5.10.4 Staff must not attempt to access any part of the Trust Network or any IT system to which they are not permitted access.

5.10.5 Access to a specific information system will be managed by the named System Administrator.

5.10.6 The Trust is required to meet the requirements set out in the NHS Care Record Guarantee. One of these requirements is for an organisation to be able to provide a full audit trail of all members of staff's access on any clinical IT systems. A patient has the right to request a copy of an audit trail, to establish who has accessed their clinical health record and the reasons for accessing their record.

5.11 Password Management

5.11.1 The Trust will adopt a standard password construction for all its information systems and where possible adopt technical measures, e.g., single sign-on to reduce the number of individual system passwords.

5.11.2 Staff must not share their passwords with any other member of staff for any reason.

5.11.3 Staff are responsible for changing their passwords when prompted and/or when they believe that their password might have been compromised.

5.11.4 Staff must ensure that they set complex passwords or pass phrases for all Trust systems they have access to, in particular systems which are available via a mobile device, e.g., phone, iPad.

5.12 Clear Screen Policy

5.12.1 The Trust has adopted a clear screen policy, which requires staff either to log off or lock their computer when left unattended.

5.12.2 Where appropriate, the Trust will implement the automatic locking of Trust computers, after a defined period of inactivity, to ensure the security of the Trust's network and its information.

5.13 Equipment Siting

5.13.1 Whenever IT equipment/IT cables are placed, consideration will be given to both the security of the IT equipment and information to be accessed on the IT equipment.

5.13.2 The correct siting of the IT equipment will reduce the risk of theft and accidental breach/disclosure of confidential information. This could occur through a member of the public being able to view confidential information displayed on the computer screen.

5.14 Procurement of IT Systems

5.14.1 Where there is an identified need for a new electronic IT system within the Trust, this must be purchased in accordance with the Trust's procurement procedures.

5.14.2 All requests for electronic systems/development must be submitted to the Trust's Digital Services Operational Group (DSOG).

5.14.3 All new IT systems must obtain IT and IG approval prior to being purchased to ensure that information security is a fundamental consideration for the IT system design and operation.

5.14.4 A Data Protection Impact Assessment (DPIA) will be undertaken against all new systems which will contain personal data. Guidance on completing these privacy impact assessments can be obtained from the Head of Information Governance or the Information Commissioner's website..

5.15 IT System Operations/Administration

5.15.1 Each Trust IT system has a named Information Asset Administrator who is responsible for overseeing the day to day security of the systems, which entails:

- ensuring that system documentation is available and kept up-to-date;
- error / system logs are reviewed and managed;
- changes to systems operations are fully tested and approved before being implemented;
- systems scheduling is planned, authorised and documented in liaison with the IT Department;
- audit logs are reviewed regularly with discrepancies investigated;
- ensuring only authorised staff or approved third parties may diagnose and correct information system hardware faults.

5.15.2 Where IT equipment or the supplier is based outside of England, the Trust will ensure Healthcare and Social Care Information Centre Off-Shore Policy is applied.

5.16 Electronic Information Management

5.16.1 The day-to-day storage of the Trust information will ensure data is readily available to authorised users.

5.16.2 Where data does not need to be readily available, the Trust will create data archives. Where information is being archived legal, regulatory and business needs must be considered.

5.16.3 The information created and stored by the Trust's information systems will be retained for a minimum period that meets both legal and business requirements in accordance with the Trust's Non-Clinical Records Management Policy.

5.17 Anti-Virus/Spyware/Malicious Code/Mobile Code

5.17.1 The Trust will purchase and run regularly updated Anti-Virus software that will be applied to all Trust IT equipment, where applicable.

5.17.2 The Trust will maintain an N3 compliant firewall which will be managed in line with this policy. Modifications made to the firewall rules will be recorded and approved by the Trust's Cyber Security Specialist and the SIRO. .

5.17.3 External organisations requiring access to Trust systems must be HSCN compliant and either hold or be working towards formal IT security certifications (e.g. Cyber Essentials, ISO 27001, Digital Marketplace).This will be checked by the Trust's Cyber Security Specialist.

5.18 Back-up, Recovery and Archiving

5.18.1 Information asset administrators must ensure there is a documented back-up and system recovery procedure in place and it is regularly tested.

5.18.2 The Trust's IM&T department is responsible for backing up the Trust servers on a daily basis in accordance with the Trust's back up procedure.

5.18.3 Staff using laptops or portable computers must ensure that these are connected to the network at least once a month to ensure that the software on the laptop is kept up to date and ensure information held is backed up (e.g., via offline folders and files).

5.18.4 The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered especially where proprietary formats are involved (e.g., means to read and recover the information must be available during the expected life of the stored information).

5.18.5 The archiving of electronic data files must reflect the needs of the Trust and any legal and regulatory requirements.

5.19 Encryption

5.19.1 To prevent the unauthorised disclosure, modification, removal or destruction of Trust information assets and disruption to the Trust business, all Trust removable media must be encrypted where it is storing personal data.

5.19.2 All Trust laptops and computers, mobile telephones, Personal Digital Assistants (PDA's) will be encrypted. Where there is an exception and a genuine business need not to encrypt a trust asset, this must be approved by the Trust's Information Governance Committee and the Trust's SIRO.

5.19.3 All Trust removable media, including but not limited to, e.g., tapes, floppy discs, removable or external hard disc drives, optical discs (DVD/CD's), solid state memory devices including memory cards and USB sticks, will be encrypted.

5.19.4 The Trust will issue staff with an encrypted USB stick where there is a business need. Information must only be stored on a Trust encrypted USB stick. Where there

is an exception to this, it must be approved by the Trust's Information Governance Committee and the Trust's SIRO. Where this is identified as a need, a risk assessment must be undertaken.

5.19.5 Removable media devices are only temporary storage devices and information must be removed from the device as soon as possible or in the case of optical media, the media destroyed. Removable media devices should only hold a secondary copy of any data, and not be the only copy in existence.

5.19.6 Where a member of staff is using non Trust equipment for Trust business/purpose, this must also be encrypted and kept secure at all times.

5.20 Security of IT Equipment

5.20.1 Where a member of staff has been issued with Trust equipment, the member of staff is fully responsible for ensuring that the Trust asset/equipment is kept secure at all times, not left unattended in a vehicle or in a public place, and locked away when not in use.

5.20.2 Staff are responsible for ensuring that all removable media are kept secure at all times to prevent their loss, damage, abuse or misuse whether stored or in transit.

5.20.3 Where staff are issued with Trust equipment, it must only be used for Trust business. Where a member of staff wishes to use Trust equipment for personal use, the member of staff must comply with all Trust policies and be approved by their Line Manager and IM&T.

5.20.4 When staff are using Trust equipment outside of the Trust, the member of staff must ensure individuals are not able to see any confidential information displayed, e.g., using laptop to access confidential information in a public place (internet café, train, café, home).

5.20.5 If any Trust equipment is lost/stolen/missing, the member of staff must immediately report the incident to the Trust through their Line Manager and, where applicable, the Police.

5.21 Uninterruptible Power Supply (UPS)/Equipment maintenance

5.21.1 The Trust has a UPS that will ensure that the systems on the Trust network are always available, except when systems maintenance is being undertaken.

5.21.2 The Trust will ensure that all IT equipment is maintained, and where new systems are purchased, a maintenance agreement is purchased to ensure the full productivity and longevity of the IT System.

5.22 Destruction of Electronic Data/hardware

5.22.1 The information stored on any media must be removed using an appropriate destruction method that makes recovery of the data impossible.

5.22.2 All data on hard drives will be permanently and securely destroyed prior to disposal.

5.22.3 Where a 3rd party is used to destroy or dispose of hard drives or assets containing personal data, the 3rd parties process will be audited by the Trust's Cyber Security Specialist and proof of secure disposal will be obtained. Only 3rd parties that hold valid accreditation will be used.

5.22.3 Where staff have electronic hardware that needs to be disposed of, this must be passed to the IT Service Desk for confidential destruction.

5.23 Forensic Readiness

5.23.1 The universal use of IT systems in the Trust leads to the need to have digital evidence available for a wide range of investigations or disputes, e.g., patient confidentiality breaches, security incidents, criminal activities, commercial disputes, disciplinary actions and privacy issues.

5.23.2 These disputes present a risk to the Trust's information assets which, without adequate mitigation, could damage the Trust's business or undermine the reputation of the Trust.

5.23.3 Where the Trust identifies a need to undertake a forensic examination, the Trust's SIRO, in liaison with the Trust's Counter Fraud Office and, HR Director will authorise such an assessment utilising the services of a commercial IT forensic company. The Trust's Head of Information Governance will secure the IT equipment following the Trust's "Removal of IT equipment procedure".

5.24 E-mail/ Intranet/Internet

5.24.1 The Management of the Trust's email system is documented in the Trust's Email Policy.

5.24.2 The management of the Trust's Internet access and intranet is documented in the Trust's Internet Policy.

5.25 Business Continuity Plan (BCP) / Disaster Recovery Plan

5.25.1 The Trust is obliged to have a BCP and Disaster Recovery Plan.

5.25.2 IM&T are responsible for undertaking a formal risk assessment in order to determine the requirements for IM&T Business Continuity and a Disaster Recovery Plan which will cover all essential and critical business activities.

5.25.3 All staff must be made aware of the Business Continuity Plan and their own related roles.

5.25.4 IM&T are responsible for keeping the IM&T Business Continuity and Disaster Recovery Plan up to date and for periodic testing to assure that the management and staff understand the plan and that it is deliverable and achieves its objective.

5.26 Personal Use

5.26.1 A limited amount of personal use of the Trust's systems is permitted subject to the following conditions:

- only undertaken during approved breaks and not during working hours;
- personal use is in compliance with this and all other applicable Trust policies/procedures, e.g., email policy, internet policy, network access procedure;
- storage of personal information is clearly identified and kept to a minimum;
- staff are not permitted to transfer, store or download any information and files for personal use including (but not limited to) MP3, AVI, WMV files and other similar formats.

5.27 Information Classification

5.27.1 NHS organisations are being encouraged to develop and adopt classification markings for all NHS information. The adoption of these categories on the Trust information systems will enable staff to easily identify the level of security required for each system.

5.27.2 There are four generic categories are proposed for NHS organisations to use:

- NHS Confidential – Patient information
- NHS Confidential - Commercial
- NHS Protect
- NHS Freedom of Information

5.27.3 The Trust will adopt these information classifications as part of the records management element of its Information Governance Work Programme.

6. DUTIES AND ORGANISATIONAL STRUCTURE

6.1 Caldicott Guardian (CG)

The **Caldicott Guardian** is the patient's advocate in that s/he is the "guardian" of patient information. Ideally, the CG must be a clinician and a member of the Board. If not on the Board, s/he must ensure that Data Protection and confidentiality matters relating to patients are raised at Board level.

6.2 Senior Information Risk Owner (SIRO)

The SIRO is the Trust's Director of Finance, who takes ownership of the Trust's information risk policy, who will act as advocate for information risk on the Trust Board and provides assurances to the Trust's Chief Executive.

The key responsibilities of the Trust SIRO are:

- Provide a focal point for managing information risks and incidents
- Take ownership of the assessment processes for information risk
- Review of the Trust's annual information risk assessment to support and inform the Statement of Internal Control
- Keep the Trust Board and Chief Executive up to date and briefed on all information risk issues affecting the organisation and its business partners

- Review and agree actions in respect of identified information risks
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution, and being appropriately communicated to all staff
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues
- Provide leadership for Information Asset Owners (IAOs) through effective networking structures, regular scheduled meetings, sharing of relevant experience, provision of training and creation of information risk reporting structures
- Advise the Board on the level of Information Risk Management performance within the Trust, including potential cost reductions/associated risks and process improvements/benefits arising etc.

6.3 Information Assets Owners (IAO)

Information Asset Owners are senior individuals involved in the running of the Trust who understand and will address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.

The key responsibilities of the Trust's IAOs are:

- understand the overall business goals of the Trust and how the information assets they own contribute to and affect these goals
- identify and document the scope and importance of all Information Assets they own
- take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks
- provide support to the Trust's SIRO and Risk Management Committee to maintain their awareness of the risks to all Information Assets that are owned by the organisation
- ensure staff are aware of and comply with expected IG working practices for the effective use of owned Information Assets
- provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets
- work closely with all other IAOs to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities.
- provide regular updates to the SIRO on the management of their Information Assets.

6.4 Information Asset Administrators (IAA)

Information Asset Administrators ensure that policies and procedures are followed as directed by the IAOs. They also:

- recognise actual or potential security incidents, and consult their IAO on incident management
- ensure that information asset registers are accurate and up to date.

6.5 Head of Information Governance

The Trust Head of Information Governance has the responsibility and role of the Trust Information Security Manager. The key responsibilities are to:

- report to the SIRO on the implementation, monitoring, documenting and communicating of information security across the Trust, to ensure compliance with UK legislation and national policy and guidance
- liaise with relevant senior/line managers on information security
- liaise with IAOs & IAAs to ensure all information assets are registered, and risk assessed with appropriate safeguards in place
- liaise with Risk Management to ensure procedures are in place for the reporting of information governance incidents, as well as monitoring actual or potential information security breaches; and ensure all identified risks and breaches are logged and handled appropriately
- liaise with the Trust's Registration Manager where changes to national/local security policy affects registration activities
- ensure the Trust's Information Security Policy is fully implemented across the Trust, so staff are aware of their responsibilities and have been trained appropriately
- develop policies and procedures that ensure the Trust has relevant and appropriate documentation in place to maintain security of all its information and information assets.

6.6 Senior/Line Management

The responsibility of Senior/Line Management is to:

- ensure all permanent and temporary staff and contractors are aware of this Information Security Policy and their security responsibilities
- ensure all staff using computer system have been trained appropriately
- ensure no unauthorised staff are allowed to access any of the Trust's computer systems or paper records
- ensure staff are given access to Trust computer systems based on their job role
- ensure all staff have fully completed the Trust employment checks
- ensure all staff leaving the Trust complete the staff leaver's procedures and return all Trust equipment
- support any information security breach investigation
- ensure all external suppliers who are contracted to supply services to the Trust have signed a Trust Confidentiality agreement, which details their legal responsibility to maintain the confidentiality of information they may come into contact with whilst working at the Trust.

6.7 Staff Responsibilities

Staff responsibilities include:

- each employed, contracted and voluntary staff member is personally responsible for ensuring that no breaches of information security result from their actions;
- attend relevant information security/governance training to ensure that are fully aware of their personal responsibilities in respect of information security, and that they are competent to carry out their designated duties;

- fully comply with the Trust's Information Security Policy and all relevant security policies and procedures;
- understand that beaches of this policy will be investigated by formal disciplinary procedure which may lead to dismissal and/or legal action;
- understand they are personally responsible for the accuracy of information/data recorded;
- ensure they are familiar with the Trust safe haven procedures for secure transportation of information;
- as part of their contract of employment, sign a formal undertaking concerning the need to protect the confidentiality of information / observe intellectual property rights of work undertaken during the terms of employment / contract, both during and after contractual relations with the Trust.

7. TRAINING/ RAISING AWARENESS / IMPLEMENTATION

7.1 All staff are mandated to attend the Trust's Information Governance training and, where appropriate, in depth information security training to ensure that they fully understand and are aware of this policy, its requirements and the obligations it places on them as a member of Trust staff.

7.2 Training for staff will include the use and protection of both paper and electronic records systems.

7.3 Training requirements will be regularly assessed and refreshed in order that staff may remain appropriately skilled/ knowledgeable over time.

7.4 Additional Information Security procedures and guidance documents will be made available to staff to support them in complying with this Policy.

8. MONITORING COMPLIANCE OF POLICY

8.1 The Trust will monitor and undertake spot checks of staff usage of the Trust network to ensure compliance with this and other related policies/procedures.

8.2 The Trust will develop and review its information security risk management programme on a regular basis to ensure its completeness, effectiveness and relevance. These reviews will be managed by the Trust's Head of Information Governance.

8.3 Where an incident occurs, either through an audit or monitoring, the Head of Information Governance will review this policy and amend where applicable.

8.4 The Trust will seek independent assurance on the compliance and application of this policy through its internal auditors and Counter Fraud Specialist.

9. EQUALITY IMPACT ASSESSMENT

9.1 This Policy has been subject to an Equality Impact Assessment and is not anticipated to have an adverse impact on any group.

10. REFERENCES

1. Department of Health Confidentiality Code of Practice 2003
2. Department of Health Records Management Code of Practice 2016
3. Department of Health Information Security Code of Practice 2007
4. Department of Health Caldicott Manual 2017
5. Department of Health Report on Information: To Share or not to Share Caldicott Review 2013.
6. Care Quality Commission – Safe Data, Safe Care, July 2016
7. National Data Guardian – Review of Data Security, Consent and Opt-Outs, July 2016
8. BS ISO/IEC 17799:2005 and BS ISO/IEC 27001: 2005 & BS7799-2: 2005
9. Data Protection Act 2018
10. General Data Protection Regulation
11. Human Rights Act 1998
12. Computer Misuse Act 1990
13. Freedom of Information Act 2000
14. Copyright, Designs and Patents Act 1988
15. Regulatory of Investigatory Powers Act 2000
16. Health and Safety at Work Act 1974
17. Health and Social Care Act 2012
18. NHS Digital – Data Security and Protection Toolkit
19. The NHS Care Records Guarantee 2006
20. The NHS IM&T Operating Framework
21. Information Commissioner's Website