South East Coast Ambulance Service NHS
NHS Foundation Trust

Information Security and Risk Management Policy

Contents

1 Introduction

1.1. The South East Coast Ambulance Service NHS Foundation Trust (the Trust) relies on high quality information to underpin the delivery of high quality evidence-based healthcare and many other key service deliverables.

1.2. An effective information security and risk management regime ensures that the Trust's information assets are properly protected, reliable and available when needed. Information has the greatest value when it is accurate, up to date and readily accessible where and when it is needed. This information applies to patient, employee and corporate records / information.

1.3. 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. All of which could compromise our ability to deliver high quality patient care.

1.4. All staff are responsible for protecting the information assets in their work area; and for reporting risks or breaches using the IRW1 incident reporting process. This policy applies to:

1.4.1. All Trust staff engaged in work for the Trust at any location, on any computer or internet connection;

1.4.2. Any other use by Trust staff which identifies the person as a staff member, or which could bring the Trust into disrepute, on any computer of internet connection;

1.4.3. Any other person working for the Trust, engaged on Trust business, or using Trust equipment and networks;

1.4.4. All usage by any person granted access to the Trust network.

1.5. The main principles underpinning the document are:

1.5.1. **Confidentiality** – access to confidential information is restricted to those with a legitimate 'need to know';

1.5.2. **Integrity** – systems operate according to the specification and to user expectations; information is recorded accurately;

1.5.3. **Availability** – information is delivered to the right person when it is needed.

1.5.4. **Security** – our network is safe, secure with controls in place.

2 Aims and Objectives

2.1. The aim of this policy is to ensure that the Trust's information assets are protected by appropriate technical and organisational measures to prevent unlawful or unauthorised processing of information; or the accidental loss, destruction or damage to data.

2.2. The objectives are to:

- Improve staff awareness of information security considerations and their legal obligations;
- Document staff responsibilities;
- Manage information security risk.

3 Definitions

3.1. **Access Controls:** the measures in place to ensure role-based access to information is available on a need to know basis.

3.2. **Information Governance Serious Incident (IG SI):** an event that places the Trust or its stakeholders at risk, such as the disclosure of confidential information to any unauthorised individual; compromise of the integrity or availability of a system or its data.

3.3. **Information Asset:** either information that is of value to the Trust or the associated hardware, software, documentation, knowledge skills or experience.

3.4. **Information Asset Owner (IAO):** An Executive Director / Head of Department responsible for managing the risks and countermeasures for the information assets within their control.

3.5. **Information Asset Administrator (IAA):** a member of staff who supports the IAO to discharge their responsibilities.

3.6. **Person-identifiable data:** information that either alone or together with other available information could lead to the identity of an individual.

3.7. **Senior Information Risk Owner (SIRO):** An Executive Director who leads and fosters a culture that manages the information risk management framework at Board level.

3.8. **Sensitive personal data:** information about an identifiable individual relating to:

3.8.1. Racial or ethnic origin;

3.8.2. Political opinions;

- Religious or other beliefs of a similar nature;
- Membership of a trade union;
- Genetic / Biometric data
- Physical or mental health or condition – Health information
- Alleged or actual criminal offences;
- Sexual orientation

3.9. **Network Security Policy:** outlines the technical and organisational controls in place to protect the confidentiality, integrity and availability of an information asset.

4 Policy Statement

4.1. Successful implementation of this policy will protect, to a consistently high standard, all Trust 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 to this policy will prevent the unauthorised disclosure, modification, removal or destruction of Trust information assets, and disruption to its business activities.

4.3. The Trust's IT and Communications systems are for business purposes only and the use of these systems are at all times subject to this policy and other named Trust policies/procedures.

4.4. This policy applies to all Trust staff and any third parties whilst contracted to provide a service to the Trust.

5 Arrangements

5.1.1. Information Risk Management

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

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

5.1.4. Data Flow Mapping of information and its flow is undertaken annually by IAA's responsible, to provide an information security risk assessment and as part of the Trust Data Protection & Security Toolkit requirements

5.1.5. This process identifies how information-related risks are controlled. Reviews of implemented information security arrangements are an essential feature of the Trust's Information Governance framework. Details of which are reported to the Trust SIRO by the Head of Information Governance via the Information Governance Working Group.

5.1.6. Once identified, information security risks will be managed on a formal basis in accordance with the Trust's Risk Management Policy and Procedure together with related procedures. The SIRO and Information Governance Working Group (IGWG) will monitor IG risks and breaches. Where appropriate, risks will be recorded within the Trust's risk register and action plans will be developed to implement risk treatment options.

5.1.7. Significant risks, meeting the criteria specified in the Risk Management Procedure will be included on the Trust's Corporate Risk Register which is reviewed by the IGWG and the Trust Board.

5.1.8. The Trust's SIRO, IAOs and IAAs will work in conjunction with the Head of Information Governance / IG Manager to manage the Trust information security risks.

5.2. **Information Assets**

5.2.1. The Trust's information assets will come in many different forms and may include:

Personal Information	Software
Patient records – manual/electronic	Clinical Systems software
Staff /Contractors records	Microsoft Office software
Clinical Audit Data	Applications software
Research Data	System Software

Management / Performance Data Trust Membership records	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	PCs/Computers Laptops / iPads 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

5.2.2. The Trust Information Asset Register will be managed and maintained by the Trust's Head of Information Governance / IG Manager in liaison with the Trust's IAOs and SIRO.

5.2.3. An information system will comprise many of the above items. Where possible the system or database will be listed as the information asset in the register and related assets will be associated with the core asset.

5.2.4. 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, email, infrastructure documentation.

5.2.5. All information assets will have:

5.2.6. An Information Asset Owner;

- Identified Information Asset Administrator(s).
- These roles will be identified when the Information Asset is entered onto the Trust's Information Asset Register.

5.2.7. 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:

5.2.8. Protection against unauthorised disclosure;

5.2.9. Integrity and evidential value of information is maintained;

5.2.10. Information is available to authorised personnel as and when it is required.

5.3. **Information Security Incident Management**

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

5.3.2. All Trust incidents must be reported using the Trust's incident reporting procedures (DIF1) and managed in line with the Trust's Incident Reporting Policy (DATIX) & Procedure, Risk Management Policy and Risk Management Procedure. All incidents must be reported as soon as they are identified.

5.3.3. Any significant IG breaches must be reported immediately to the Head of Information Governance / IG Manager.

5.3.4. Where there is an information security breach or event, this will be reported to the Trust's Head of Information Governance / IG Manager who will inform the Trust's SIRO and/or Caldicott Guardian.

5.3.5. The Trust's SIRO will review reported information security incidents and where applicable recommend or approve changes to Trust policies and procedures respectively to reduce the risk of the information security incident reoccurring.

5.3.6. Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals will be considered as serious and may be reported as an IG Serious Incident. This applies irrespective of the media involved and includes both the loss of electronic media and paper records.

5.3.7. Information security breaches classified as an IG SI will be reported via the DoH STEIS system and other relevant bodies as outlined in Department of Health guidance.

5.3.8. IG SI's must be reported to the ICO and recorded on the Data Security & Protection Toolkit. IG SI's must be reported immediately to the Head of Information Governance / IG Manager

in order for the Trust to meet its 72 hour statutory reporting timeframes.

5.4. **Security of Manual/Verbal Information**

5.4.1. **Safe Havens**

5.4.2. The definition of a safe haven is a secure location where a designated member of staff is responsible for ensuring the secure receipt and delivery of information sent to the Safe Haven. The Trust's Safe Haven arrangements are detailed in its Transmission and Secure Storage of Confidential Information (Safe Haven) Policy.

5.4.3. The faxing confidential / patient information must only be used in **exceptional circumstances**. This is not the most secure method of transferring information and other methods must be considered. Before faxing confidential information staff, must consider alternative methods for transferring information e.g. Encryption of SECAmb email, NHS mail (nhs.net accounts), post, encrypted removable media.

5.4.4. If a fax is received in error the recipient must immediately advise the sender. The document must not be disclosed and securely destroyed using the Trust approved confidential waste facility. The recipient must then inform the sender that the document has been securely destroyed and raise a DIF-1 form.

5.4.5. **Verbal Information**

5.4.6. The Trust has a legal obligation to ensure that all personal data being processed is kept securely in accordance with Data Protection legislation.

5.4.7. Staff must ensure that confidential conversations are not undertaken in a public / open work area, or where those who do not need to access to the confidential information can overhear the conversation.

5.4.8. Where answer phones are used, consideration must be given to where they are sited and who may access the messages in order to maintain confidentiality. PIN access to messages must be used where possible.

5.4.9. The identity of persons requesting and/or receiving sensitive or confidential information over the telephone must be verified along with their authority to access the information.

5.4.10. All staff must be aware that telephone lines in the Emergency Control Rooms and Clinical Scheduling offices are recorded and

may be accessed by authorised staff in certain circumstances in accordance with the terms of The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

5.4.11. Similarly, all communications sent or received via Trust email, Skype for business, SMS, digital radio, Communicator etc are stored on Trust servers and may be accessed as described above.

5.4.12. **Confidential Paper Records**

5.4.13. Confidential paper based records must not be left unattended in an insecure area. Filing cabinets must be locked or secured in a locked room where physical access controls are in place.

5.4.14. When paper records require destruction, they must be placed in the confidential waste units provided by the Trust or shredded on Trust premises.

5.5. **Clear Desk Policy**

5.5.1. All staff must ensure that all confidential information is secured and removed to a secure location e.g. locked filing cabinets if unattended.

5.6. **Sharing Confidential Information**

5.6.1. Where there is a need for staff to share patient information with another NHS organisation, they must ensure that this complies with both the Data Protection Act 2018, General Data Protection 2016, and the Common Law Duty of Confidentiality.

5.6.2. Sharing confidential information must also comply with the Caldicott principles and the framework set out in the appropriate Information Sharing Protocols that the Trust has signed up to; as well as Trust policies and procedures.

5.7. **Security of Electronic Information**

5.8. **Access Control**

5.8.1. 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 access to authorised individuals to meet business needs. Access controls will be issued on a strictly need to know basis and in accordance with legislation and regulation.

5.8.2. Access to the Trust's Network is documented in the Trust's Network Security Policy.

5.8.3. Line managers will use the staff changes process to inform HR of starters, leavers and those who change their role or base.

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

5.8.5. Access to a specific information system will be managed by the named IAO or IAA

5.8.6. 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 trial of all staff's access on any clinical IT systems. A patient / employee has the right to request a copy of an audit trail, to establish who has accessed their clinical health record and the reasons for access.

5.8.7. Arrangements for staff with a requirement to access the Trust networks remotely are documented in the Trust's Remote Access Policy.

5.8.8. Third party access to information assets will only be granted once a formal contract has been signed that contains the necessary controls to minimise the risk to information security.

5.9. **Password Management**

5.9.1. The IT Department will agree password management policies for the different IT systems and where possible will adopt technical measures e.g. single sign-on, to reduce the number of individual system passwords.

5.9.2. Passwords will not be displayed on the screen when entered.

5.9.3. Staff must not share their passwords, for any reason or leave a written record of their passwords in a format that others may access.

5.9.4. Staff are responsible for changing their passwords when prompted and for choosing 'strong' passwords which contain a mixture of upper and lowercase letters, numbers and/or symbols.

5.10. **Smartcards**

5.10.1. Sharing Smartcards is strictly forbidden. Staff who contravene this condition will be subject to a disciplinary investigation in accordance with Trust policy.

5.11. **Clear Screen Policy**

5.11.1. Whenever a member of staff leaves their computer unattended, they must either lock their screen, log off or shutdown their computer. Where workstations are shared, staff must log off rather than lock the screen.

5.11.2. Where appropriate, the Trust will implement the automatic locking of Trust computers, after a defined period of inactivity.

5.12. **Location of Equipment**

5.12.1. Whenever IT equipment/IT cables are placed, consideration will be given to health and safety factors as well as the security of the IT equipment and information to be processed on it.

5.12.2. Locating IT equipment appropriately will reduce the risk of theft and accidental breach/disclosure of confidential information. The latter could occur through a member of the public being able to view confidential information displayed on the computer screen.

5.13. **Procurement of IT Systems**

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

5.13.2. 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.

5.13.3. A Data Protection Impact Assessment must be undertaken at an early stage when new systems or processes are planned that contain or affect personal data. Guidance on completing these Data Protection Impact Assessments can be obtained from the staff intranet which provides a template, the Information Commissioner website or the Trust's Head of Information Governance / IG Manager.

5.13.4. The Head of Information Governance / IG Manager holds a centralised repository of all Data Protection Impact Assessment forms which have been completed.

5.14. IT System Operations/Administration

5.14.1. Each Trust IT system has at least one IAA who is responsible for overseeing the day to day security of the systems. This entails:

5.14.2. 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.

- Where IT equipment or the supplier is based outside of England, the Trust will ensure NHS Digital Off-Shore Policy is applied.

5.15. **Electronic Information Management**

5.15.1. The day-to-day storage of information on the Trust's network will ensure data is readily available to authorised users.

5.15.2. 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.

5.15.3. The information created and stored by the Trust's information systems must be retained for a minimum period that meets both legal and business requirements in accordance with the Trust's Records Management Policy and Procedure. Reference must be made to the Records Management Code of Practice for Health and Social Care 2016 published by the Information Governance Alliance (IGA)

5.16. **Anti-Virus/Spyware/Malicious Code/Mobile Code**

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

5.16.2. 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.

5.16.3. External organisations requiring access to Trust systems must be have an Information Governance Statement of Compliance (SOC) and satisfactory Data Security & Protection Toolkit scores, which will be checked by the Trust IG Manager on an annual basis as part of the Data Security & Protection Toolkit Assessment.

5.17. **Back-up, Recovery and Archiving.**

5.17.1. IAAs must ensure that documented adequate back-up and system recovery procedures are in place and regularly tested.

5.17.2. The Trust's IT department is responsible for backing up the Trust servers on a daily basis in accordance with the relevant System Level Security Procedure.

5.17.3. 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).

5.17.4. Staff who have been provided with a Trust issued EPCR iPad must ensure that any software updates are installed.

5.17.5. 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 store information).

5.17.6. Archiving electronic data files must reflect the needs of the Trust and any legal and regulatory requirements.

5.18. **Encryption**

5.18.1. To prevent the unauthorised disclosure, modification, removal or destruction of Trust information assets and disruption to the Trust business, all Trust equipment and removable media will be encrypted where possible regardless of the data that is stored on them.

5.18.2. All Trust laptops, iPads, Smartphones, Personal Digital Assistants (PDAs) or other similar equipment will be encrypted. Where there is an exception and a genuine business need to not encrypt a Trust asset, this must be approved by the Trust's SIRO and reported to the IGWG.

5.18.3. All Trust removable media including, but not limited to e.g. tapes, removable or external hard disc drives, solid state memory devices including memory cards and USB sticks, must be encrypted.

5.18.4. The IT Department 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. Exceptions to this must be risk assessed and approved by the Trust's IGWG and the SIRO.

5.18.5. 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.

5.18.6. Staff must not use personal IT equipment for business purposes unless there is an identified exceptional need that has been risk assessed and approved by the Trust's IGWG and the SIRO.

Confidential information must not be processed on such equipment unless the device is encrypted to NHS standards.

5.19. **Security of IT Equipment**

5.19.1. 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.

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

5.19.3. Where staff are issued with Trust equipment, it must normally 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 have permission from their line manager.

5.19.4. Staff who have been provided with a Trust issued EPCR iPad are able to use this for personal use provided that usage is in line with the Trust Mobile Devices policy .

5.19.5. 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 e.g. using laptop / iPad / Smartphone to access confidential information in a public place (internet café, train, café, home).

5.19.6. If any Trust equipment is lost/stolen/missing the member of staff must report the incident to the Trust immediately to the IT Department, and follow the Trusts defined incident reporting arrangements, and where applicable to the Police.

5.20. **Uninterruptible Power Supply (UPS)/Equipment maintenance**

5.20.1. The Trust has UPS and failover mechanisms in place to ensure that the Trust's critical systems are always available, except when systems maintenance is being undertaken.

5.20.2. 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.

5.21. **Destruction of Electronic Data/hardware**

5.21.1. The information stored on media must be removed using a destruction method that makes recovery of the data impossible.

5.21.2. All data on hard drives will be permanently erased by IT and removed from Trust equipment before being handed to Trust's third party contractor for confidential destruction.

5.21.3. Where staff have electronic hardware that needs to be disposed, this must be passed to the IT Service Desk for confidential destruction. Media destruction bins (e.g. CDs, floppy discs, memory sticks) have been located at the Trusts main sites and their locations have been circulated to the Trust.

5.22. **Forensic Readiness**

5.22.1. 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 / employee confidentiality breaches, security incidents, criminal activities, commercial disputes, disciplinary actions and privacy issues.

5.22.2. 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.

5.22.3. Where the Trust identifies a need to undertake a Forensic examination, the Trust's SIRO, in liaison with the Trust's Local Counter Fraud Specialist and Director of Human Resources, will authorise such an assessment utilising the services of a commercial IT Forensic company. The Trust's Head of Information Governance / IG Manager or Head of IT will secure the IT equipment.

5.23. **E-mail/ Intranet/Internet**

5.23.1. The management of the Trust's internet and email system is documented in the Trust's Internet and Email Policy.

5.24. **Business Continuity Plan (BCP) / Major Incident Plan**

5.24.1. The Trust must have a BCP and Major Incident Plan.

5.24.2. IT are responsible for undertaking a formal risk assessment in order to determine the requirements for IT Business Continuity which in liaison with the Trust's Business Continuity and Disaster Recovery covers all essential and critical business activities.

5.24.3. Staff must be made aware of the Business Continuity Plan and their own related roles.

5.24.4. IT are responsible for keeping the IT 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.

5.25. **Personal Use**

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

5.25.2. Only undertaken during approved breaks and not during working hours.

5.25.3. Personal use is in compliance with this and all other applicable Trust policies/procedures e.g. internet and email policy, Code of Professional Conduct and does not breach relevant legislation, such as the Computer Misuse Act 1990.

5.25.4. Storage of personal information is clearly identified and kept to a minimum.

5.25.5. Staff are not permitted to transfer, store or download of any information and files for personal use including (but not limited to) MP3, AVI, WMV files and other similar formats.

5.26. **Information Classification**

5.26.1. 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 and records will enable staff to easily identify the level of security required for each.

5.27. The Trust will adapt the NHS and Cabinet Office Civil Contingencies Secretariat (CCS) classification schemes to develop one that recognises that, as a Cat 1 responder, the Trust has to incorporate some of the CSS categories that are excluded from the NHS scheme.

5.28. This guidance will be published separately and will be adopted as part of the records management element of its Information Governance Work Programme which is approved by IGWG

6 Responsibilities

6.1. **Overview**

6.1.1. Responsibility for information security resides, ultimately, with the Trust's Chief Executive Officer. Operational responsibility for this has been delegated to the Executive Director of Strategy & Business Development who is the Trust's Senior Information Risk Owner (SIRO).

6.1.2. The SIRO is supported by Information Assets Owners (IAOs) who are the Heads of Department; and their Information Asset Administrators (IAAs).

6.1.3. The IAOs are responsible for ensuring that their information assets are managed appropriately and providing assurance to the Trust's Senior Information Risk Owner (SIRO). The SIRO in turn will provide assurance to the Trust's Chief Executive Officer and Trust Board.

6.1.4. IAOs will be supported by Information Asset Administrators (IAAs), who are staff with day to day responsibility for managing the information asset e.g. clinical, financial or staff systems.

6.1.5. The Trust's Head of Information Governance / IG Manager is responsible for managing and implementing this policy and related procedures to maintain the security of all information held by the Trust. This will be achieved in conjunction with the Trust's Information Asset Owners and Administrators.

6.2. **Specific responsibilities**

6.2.1. The **Chief Executive Officer,** as the Trust's Accountable Officer, has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

6.2.2. The **Senior Information Risk Owner (SIRO)** is the Trust's Executive Director of Strategy & Business Development who provides the focus for the management of information risk at Board level. The key responsibilities of the Trust SIRO are to:

6.2.3. lead and foster a culture that values, protects and uses information effectively for the benefit of the Trust and its stakeholders; providing leadership for IAOs through effective networking structures, provision of training and creation of information risk reporting structures;

6.2.4. own the Trust's information risk and incident management framework; review risk assessments and provide a focal point for the escalation, resolution and/or discussion of information risk issues;

6.2.5. own the Trust's overall Information Security and Risk Management Policy and risk assessment processes and ensure they are implemented by the IAOs;

6.2.6. review the Trust's annual information risk assessment to support and inform the Annual Governance Statement

6.2.7. brief the Trust Board and Chief Executive Officer on information risk issues affecting the organisation and its business partners.

6.2.8. The **Information Assets Owners (IAOs)** are Heads of Department They understand and will address risks to the information assets they 'own' and provide assurance to the SIRO on the security and

use of those assets. The key responsibilities of the Trust's IAOs are to:

6.2.9. understand the overall business goals of the Trust and how the information assets they own contribute to and affect these goals;

6.2.10. identify and document the scope and importance of all Information Assets they own;

6.2.11. be accountable for the 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;

6.2.12. support the Trust's SIRO by implementing and monitoring the Trust's information risk management processes; and providing regular updates on the management of their Information Assets;

6.2.13. ensure staff are aware of and comply with expected IG working practices for the effective use of owned Information Assets;

6.2.14. work closely with all other IAOs to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities; and

6.2.15. **Information Asset Administrators (IAA)** are members of staff responsible for managing information assets at an operational level. Their key responsibilities are to support their IAO by:

6.2.16. ensuring that policies and procedures are followed;

6.2.17. recognising actual or potential security incidents; consulting their IAO on incident management; and

6.2.18. ensuring that information asset registers are accurate and up to date.

6.2.19. The **Caldicott Guardian**, the Trust's Medical Director, champion's patient interests at Board level and will review risk and incidents relating to patient information/systems.

6.2.20. **The Head of Information Governance** / **Information Governance Manager** will:

6.2.21. provide support and advice to the Caldicott Guardian, SIRO and IAOs;

6.2.22. review information security risks and incidents liaising with the Caldicott Guardian, SIRO and IAOs as appropriate;

6.2.23. liaise with the Head of Compliance where IG SIs are identified.

6.2.24. The **Head of Information Governance / IG Manager** will report IG SIs in accordance with Department of Health / Information Commissioners Officer guidance.

6.2.25. The **Head of IT** is responsible for providing technical support to IAOs and implementing this policy in relation to information held within the Trust's electronic systems.

6.2.26. **Line Managers** are responsible for ensuring that:

6.2.27. all their permanent or temporary staff and contractors are aware of this policy and their security responsibilities;

6.2.28. their staff are trained in the use of the relevant computer systems;

6.2.29. role based access to systems and information is strictly applied; and changes in personnel or roles are notified through the appropriate channels;

6.2.30. they support or undertake investigations into information security breaches;

6.2.31. all external suppliers who are contracted to supply services to the Trust have signed confidentiality agreements, detailing their legal responsibility to maintain the confidentiality of information they may come into contact with whilst working for the Trust.

6.2.32. **All staff** have a responsibility to:

- adhere to Trust policies and procedures to protect the information and systems that they use;
- ensure that information within their control is appropriately protected, timely, accurate, up to date and available to authorised users when needed;
- undertake mandatory IG training as identified in the training needs analysis for the appropriate financial year;
- report information security risks and incidents;
- understand that breaches of this policy may be investigated under the Disciplinary Policy and Procedure and could lead to dismissal and/or legal action.

7 Competence

7.1. Staff will undertake training appropriate to their role as identified in the Trust's IG training needs analysis.

7.2. Staff will be required to complete and pass the mandatory – Induction and subsequent IG Refresher Training and Assessment on an annual basis in each financial year.

8 Monitoring

8.1. IAOs are responsible for monitoring compliance with this policy in relation to their own information assets. This may take the form of spot checks, monitoring information security incidents and/or risk assessments.

8.2. The Head of Learning and Development via the L&D Resource co-ordinator will provide the uptake of IG training reports to the Head of Information Governance / IG Manager.

8.3. The Head of Information Governance / IG Manager will provide an IG Training monitoring report / completion update for each IGWG meeting. The Head of Information Governance / IG Manager will provide reports of risks and incidents identified to the SIRO and Caldicott Guardian for discussion and resolution at their bi-monthly meetings. The Head of Information Governance / IG Manager will inform them immediately of any significant breaches.

8.4. The IGWG will monitor the IG risks and incidents log at each of its meetings meeting.

8.5. The Head of Information Governance / IG Manager will provide reports on IG compliance and risk to each IGWG meeting.

9 Audit and Review

9.1. The Trust will seek independent assurance annually from its auditors on the compliance and application of this policy.

9.2. This policy will be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced or a significant information security risk or event occurs that indicates a review is required.

9.3. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

9.4. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

9.5. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

10 Equality Impact Analysis

10.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

10.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those function.

11 References

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Caldicott Principles
- Confidentiality: NHS Code of Practice, DH, 2003
- Confidentiality: NHS Code of Practice - supplementary guidance: public interest disclosures, DH, 2010
- Records Management Code of Practice for Health and Social Care 2016
- Information Security: NHS Code of Practice, DH, 2007
- Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents, DH (Gateway ref:13177),

- BS ISO/IEC 27001:2005 Information technology – Security techniques — Information security management systems — Requirements

- BS ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management