



## Information Security Policy

Document Profile Box	
Document Category / Ref	QSSD 1322
Version:	0001
Ratified by:	Policy Review Group Trust Board
Date ratified:	24 <sup>th</sup> September 2009
Name of originator / author:	Rahima Hoque – Information & Service Modelling Manager
Name of responsible committee / individual:	Information Governance Working Group
Date issued:	31 <sup>st</sup> October 2009
Review date:	1 year from issue date
Target audience:	All staff
Document owner:	Colin Cessford – Director of Strategy and Business Development
Approved by:	

## Version Control

Version	Release Date	Author	Status	Comments
0000.1	Apr 2009	Rahima Hoque	Draft	First draft
0001	Oct 2009	Rahima Hoque	Final	

### Did you print this document yourself?

Please be advised that the Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version.

### Document Location

The source of the document will be found in the Trust Quality System.

### Freedom of Information Act 2000 Access

This document will be available via the NEAS Publication Scheme.

## TABLE OF CONTENTS

	<b>PAGE</b>
1. INTRODUCTION	1
2. PURPOSE	2
3. SCOPE	2
4. DEFINITIONS	3
5. RESPONSIBILITY AND ACCOUNTABILITY	4
6. EQUALITY AND DIVERSITY STATEMENT	7
7. LEGAL AND PROFESSIONAL OBLIGATIONS	8
8. INFORMATION ASSETS	9
9. INFORMATION CLASSIFICATION	10
10. ACCESS CONTROL	13
11. MONITORING SYSTEM ACCESS AND USE	14
12. REMOTE ACCESS	15
13. EXCHANGES OF INFORMATION AND SOFTWARE	16
14. SYSTEMS DEVELOPMENT AND MAINTENANCE	16
15. INCIDENT AND RISKS	17
16. DISASTER RECOVERY PLAN	17
17. CONSULTATION, APPROVAL AND RATIFICATION PROCESS	17
18. REVIEW AND REVISION ARRANGEMENTS	18
19. DISSEMINATION AND IMPLEMENTATION	18
20. DOCUMENT CONTROL INCLUDING ARCHIVING ARRANGEMENTS	18
21. MONITORING COMPLIANCE WITH AND THE EFFECTIVENESS OF PROCEDURAL DOCUMENTS	19
22. REFERENCES	20

## 1. Introduction

- 1.1. The policy has been developed to protect, to a consistently high standard, all information assets, including patient records and key information services, to meet the statutory requirements set out within the Data Protection Act 1998 (DPA) and to satisfy our obligations under the Civil Contingencies Act 2004.
- 1.2. This policy is intended to define what the term “information” relates to, to inform all staff of their responsibilities in relation to correct use and management of information and offer help to staff in how to achieve and maintain the required security standards.
- 1.3. It is essential that all of the North East Ambulance Service (NEAS) systems are protected to an adequate level from business risks. Such risks include accidental data change or release, malicious user damage, fraud, theft, failure and natural disaster. It is important that a consistent approach is adopted to safeguard the Trust’s information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.
- 1.4. Without effective security, NHS information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties.
- 1.5. Inaccurate, outdated or inaccessible information that is the result of one or more information security weaknesses can quickly disrupt or devalue mission critical processes, and these factors should be fully considered when commissioning, designing or implementing new systems. An effective information security management regime, therefore, ensures that information is properly protected and is reliably available.
- 1.6. NHS information may be needed to:
  - Support patient care and continuity of care.
  - Support day-to-day business processes that underpin the delivery of care;
  - Support evidence-based clinical practice.
  - Support public health promotion and communicate emergency guidance.
  - Support sound administrative and managerial decision making, as part of the knowledge base for the NHS.
  - Meet legal requirements, including requests from patients under the provisions of the DPA or the Freedom of Information Act (FOI).
  - Assist clinical or other types of audit.
  - Support improvements in clinical effectiveness through research.
  - Support archival functions by taking account of the historical importance of information.
  - Support patient choice and control over treatment and services designed around patients.

## 2. Purpose

- 2.1. The purpose of this document is to set out a framework under which the policy will preserve confidentiality, integrity and availability of information.
- 2.2. It is essential that all information processing systems are protected from events which may jeopardise the activities of NEAS. These events will include accidents as well as behaviour deliberately designed to cause difficulties. Adherence to this policy and related policies and procedures, will ensure that the risk of such occurrences is minimised.
- 2.3. This policy aims to raise the awareness of all Trust employees, Contractors and Third Party Suppliers of the need to maintain and where necessary improve the security and confidentiality of systems and data.
- 2.4. Finally this policy is a means through which information security issues and their impact can be disseminated throughout the Trust to all staff.

## 3. Scope

- 3.1. This policy covers all aspects of information within the Trust including:
  - Information systems
  - Networks
  - Applications
- 3.2. Information assets may consist of:
  - Digital or hard copy patient health records.
  - Digital or hard copy administrative information (including, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records).
  - Digital or printed, photographs, slides, outputs and images.
  - Digital media (including, for example, data tapes, CD-ROMs, DVDs, USB / Flash disk drives, removable memory stick devices and all other internal or external media compatible with NHS information systems.
  - Computerised records, including those that are processed in networked, mobile and standalone systems.
  - E-Mail, text and other message types.

*(Adapted from DOH Information Security Management: NHS Code of Practice)*

- 3.3. This policy covers all sites and systems operating and utilised by NEAS.
- 3.4. The policy applies to any individual employed, in any capacity, by the Trust.
- 3.5. Any breach of the policy is considered to be an offence and in that event, NEAS disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Trust, and who have access to personal information, will be expected to have read

and comply with this policy. It is expected that departments / sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

#### **4. Definitions**

- 4.1. **Personal data** is data which relate to an individual who can be identified from those data or from those data and other information which is in the possession of, or likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any person in respect of the individual. Personal information includes name, address, date of birth, or any other unique identifier such as NHS Number, hospital number, national insurance number etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode etc.
- 4.2. **Sensitive personal data** is defined in Section 2 of the DPA as data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. These data are subject to more stringent conditions on their processing when compared to personal information.
- 4.3. **System or data** used in the context of this policy refers to all information held in either electronic or paper format, also an "information asset" is a definable piece of information stored in a manner which is recognised as 'valuable' to the Trust.
- 4.4. **Encryption** is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.
- 4.5. **External hard drive** sits outside the main computer in its own enclosure. This portable encasement allows the user to store information on a hard drive that is not part of the computer, but is connected via a high-speed interface cable normally a USB or firewire.
- 4.6. **Hardware** in Information Technology is a physical device such as a VDU or printer.
- 4.7. **Patches** are updates to computer programs, such as anti virus, to keep the program up to date or to fix a bug within a program.
- 4.8. **PDA, personal digital assistant**, refers to a handheld device that has several features including an address book, contacts list, calendar and memo and note pad e.g. Blackberry.
- 4.9. **Removable media** is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs / DVDs, USB flash memory sticks or pens, PDAs.
- 4.10. **Smartcard** is any plastic card (like a credit card) with an embedded microchip for storing information. The NHS smartcard is used to control security access to electronic patient records.

- 4.11. **Software** are programs that run on a computer e.g. word-processing software, spreadsheets etc.
- 4.12. **USB, universal serial bus or port connection** that is universally compatible with many types of device such as wireless, printers, memory sticks etc.
- 4.13. **USB memory sticks** are devices with flash memory card formats. These devices come in many sizes and are generally used for the storage of data.

## 5. Responsibility and Accountability

5.1. Responsibility for Information Security rests with the Chief Executive. Information security on a day to day basis is the responsibility of the Trust's Information Governance Lead, with support from the IT Manager and the Risk Manager. However, complying with the requirements of information security is an organisation-wide responsibility.

5.2. Duties within the Organisation.

### 5.2.1. All staff have a responsibility to:

#### *General*

- Comply with security procedures.
- Maintain data confidentiality and integrity.
- Undertake training in line with the requirements of their role.
- Bring to their line manager or security lead areas of concern around information security.
- Ensure the operational security of all systems they use and that there is no breach in information security as a result of their actions.

#### *Equipment disposal*

- Ensure the IT Service Desk is informed of any IT equipment that needs to be disposed of. Under no circumstances must staff pass on or dispose of equipment themselves.

#### *Physical security*

- Ensure doors and windows are locked and secured when the area is left unattended in areas where IT equipment is in use.
- Ensure all portable equipment is secured when not in use.
- Do not leave equipment or removable media unattended when travelling.
- Do not leave portable media laptops when travelling in case of theft.
- Ensure that unattended PCs / laptops have appropriate protection e.g. log-off, lock screens or use password-protected screen saver.

#### *Information security*

- Store information on networked drives that are subject to authorisation and access controls, and not on the C drives.

- Ensure that appropriate security measures are in place for non networked computers to protect the information held on these.
- Sensitive or confidential information, when printed, will be removed from printers, photocopiers and fax machines immediately.
- Where information is transferred by fax, appropriate measures will be taken to ensure that there is no accidental disclosure.
- Safe haven procedures are followed when transferring personal or sensitive information.

#### 5.2.2. **Line managers have a responsibility to:**

##### *General*

- Ensure all current, new, temporary staff and contractors are instructed in their responsibilities in relation to information security policy and procedures and work in a manner consistent with this policy.
- Ensure staff using computer systems are appropriately trained in their use.
- Ensure that the IT Service Desk are notified of new and leaving employees to allow access rights to be appropriately established from effective dates and leaving employees access to be revoked.
- Investigate and take relevant action on any potential breaches of this policy supported by security leads and the Information Governance Working Group (IGWG) in line with existing risk management procedures.

##### *Information security*

- Ensure that no unauthorised staff are allowed to access any of NEAS computer systems or information stores as such access could compromise information integrity.
- Ensure that staff not employed by the trust e.g. contractors, students etc. have signed appropriate confidentiality agreements before accessing IT equipment.
- Determine which individuals are to be given authority to access specific information: levels of access to specific systems should be based on job function, independent of status.
- Decide whether it is appropriate for their staff to use private equipment e.g. PDA's, external hard drives, USB memory sticks. This will include considering whether it is needed to carry out their duties and whether it may pose a confidentiality or security risk.
- Ensure that exit interviews are conducted and relevant accounts closed and equipment returned via HR and IT Service Desk.

#### 5.2.3. **The NEAS IGWG have a responsibility to:**

- Developing, maintaining and implementing the Information Security Policy and procedures across NEAS ensuring that they meet national and legislative requirements in relation to information security.

- Monitoring progress of information security against the Information Governance Toolkit (IGT).
- Developing standards and guidance relevant to information security.
- Promoting awareness of information security issues.
- Ensuring information security risks and incidents are identified, logged, actioned and monitored routinely.
- Other sub groups will also work on specific areas relating to information security including confidentiality and data quality.

#### 5.2.4. Information Security Lead(s) have a responsibility to:

##### *General*

- Monitor and report on the state of information security within the Trust.
- Develop and enforce detailed procedures to maintain security.
- Ensure that Trust personnel are aware of their responsibilities and accountability for information security.
- Provide advice on information security when required.
- Assess the impact on IT provision of any major disruption and invoke appropriate action as per any disaster recovery plans.
- Implement adequate processes to ensure that third parties with whom the Trust contracts are subject to, and comply with, information security requirements.

##### *Information security*

- Monitor for actual or potential information security breaches.
- Report information security issues in line with the NEAS IGWG Terms of Reference.
- Understand the risk to the computer assets and the information that is held on them.
- Implement specific security measures where personal information is being transferred whether manually or electronically e.g. using portable computers, USB etc.
- Ensure access controls are established and maintained for all staff to ensure appropriate access to information.
- Commission penetration testing to ensure network security.
- Ensure back up procedures are established and maintained.

##### *Physical security*

- Deploy appropriate security measures to reduce the threat and to reduce the impact of a threat that materialises.
- Ensure that new information systems provide an adequate level of security and do not compromise the existing infrastructure.

- Ensure appropriate revision of antivirus software and patches are installed on all servers and PCs.
- Produce and maintain an IT asset register for software and hardware used by Trust staff.
- Ensure server rooms are restricted to appropriate staff members.
- Ensure all critical equipment is protected from power supply failures and bursts using Uninterruptible Power Supplies (UPS) and UPS' are tested on a regular basis.
- Ensure that PCs, servers and other relevant hardware is disposed of securely in accordance with disposal legislation.

**5.2.5. HR has a responsibility to:**

- Ensure necessary screening of staff is carried out through the recruitment process.
- Ensure every contract references employee's responsibilities with regard to information security and make it clear that employees are required to comply with the Trust policies.
- To ensure exit interviews procedures incorporate appropriate security points e.g. removal of nhs.uk / nhs.net accounts, pass codes etc via line managers and IT Service Desk.
- Individuals who are not employed or contracted to The Trust but who have access to or may come into contact with confidential information will sign an appropriate confidentiality agreement before access is permitted. For example this would apply to voluntary staff that may have access to confidential information. The agreement will be signed, dated and the original returned to The Trust before access is granted.

**6. Equality and Diversity Statement**

- 6.1. All public bodies have statutory duties under the Race Relations (Amendment) Act 2000, the Disability Discrimination Act 2005 and the Equality Act 2006 to set out arrangement to assess and consult on how their policies and functions impact on race, gender and disability equality, in effect to undertake Equality Impact Assessments (EIA) on all policies / guidelines and practices.
- 6.2. Best practice also suggests that the EIA should be extended to include equality and human rights with regard to age, religion and sexual orientation.
- 6.3. The Trust is committed to providing equality of opportunity, not only in its employment practices but also in the services for which it is responsible. As such, this document has been screened, and if necessary an EIA has been carried out on this document, to identify any potential discriminatory impact.
- 6.4. If relevant, recommendations from the assessment have been incorporated into the document and have been considered by the approving committee. The Trust also values and respects the diversity of its employees and the communities it serves. In applying this policy, the Trust will have due regard for the need to:

- Eliminate unlawful discrimination.
- Promote equality of opportunity.
- Provide for good relations between people of diverse groups.
- For further information on this, please contact the Equality and Diversity Department.

## **7. Legal and Professional Obligations**

- 7.1. The Trust regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.
- 7.2. The key statutory requirement for NHS compliance with information security management principles is the DPA, and in particular its seventh principle. The Act provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer. It applies to personal information generally, not just to health records, and therefore the same principles apply to records of employees held by employers, for example in finance, human resources and occupational health departments.
- 7.3. Non-personal, non-confidential information on NEAS and its services should be available through a variety of media in line with the Trust's FOI Publication Scheme.
- 7.4. The Trust will ensure that any transfers of personal information outside of the European Economic Area are only completed when sufficient security exists within the receiving country.
- 7.5. The Trust will undertake or commission regular audits to assess its compliance with legal requirements.
- 7.6. NEAS will comply with the following legislation and other legislation as appropriate:
  - The Data Protection Act (1998)
  - The Data Protection (Processing of Sensitive Personal Data) Order 2000
  - The Copyright, Designs and Patents Act (1988)
  - The Computer Misuse Act (1990)
  - The Health and Safety at Work Act (1974)
  - Human Rights Act (1998)
  - Regulation of Investigatory Powers Act 2000
  - Freedom of Information Act 2000
  - Health & Social Care Act 2000
  - Fraud Act 2006
  - Crime and Disorder Act (1998)
  - Access to Health Records Act (1990)

## **8. Information Assets**

8.1. There are six major categories of information assets including information, software, physical (including hardware), services, people and other less tangible assets such as reputation and image of the Trust. The key assets that this policy applies to are information, hardware and software.

### **8.2. Asset register**

A complete IT asset register which will include key hardware, software and information assets will be developed by the IT Department and will be maintained by the asset owners. Procurement of any new assets must be recorded in the asset register and allocated an appropriate owner. Disposal of assets or the reassignment of assets must be recorded in the asset register. Each asset shall have a named custodian who shall be responsible for the information security of that asset.

8.2.1. The asset inventory will as a minimum identify:

- The item.
- Its security classification.
- The owner of the asset.
- The location of the asset.
- The type of media (if the asset is data).
- The date of entry to the inventory.
- The date of removal.

8.2.2. For the purposes of security, one 'owner' will be appointed for each convenient logical or physical set of assets, for example: the System Owner or Head of Department together with an IT Technical Lead. This owner and IT Technical Lead will be responsible for:

- Identifying information assets within the area of responsibility.
- Specifying in terms of security what the asset can be used for.
- Determining who can use the asset.
- Approving appropriate security protection for the asset.
- Ensuring compliance with the security controls.
- Risk management and accreditation of assets.

8.2.3. Information assets will also be maintained in a register similar to that of the IT asset register and will contain key information assets which have business value.

### **8.3. Hardware and software**

8.3.1. Users requiring equipment to carry out authorised tasks are to apply for equipment and funding through department heads. Purchase of this equipment will then be carried out centrally by IT. This ensures that equipment purchased is compatible with existing systems.

- 8.3.2. Any new software must be authorised by IT. Unauthorised software is prohibited on the NEAS network. The organisation shall ensure that all information products are properly licensed and users shall not install software on the organisation's property without permission from the IT Department. Users breaching this requirement may be subject to disciplinary action.
- 8.3.3. Users will not modify the equipment. Such modifications that are required to ensure the efficiency of the PC will be provided and installed by IT staff (within budgetary constraints).
- 8.3.4. Private equipment will not be used for the purpose of carrying out Trust business without prior permission from the individual's line manager. This private equipment may include laptops, PDA's, USB memory sticks and external hard drives.
- 8.3.5. It will be the responsibility of the line manager to decide if this is necessary for the person to carry out their duties or whether it may pose a confidentiality or security risk.
- 8.3.6. The IT Department maintains IT hardware and software. The user will not authorise any maintenance to be carried out by any other agency.
- 8.3.7. Users are responsible for ensuring their information is saved appropriately and subject to regular backup. Where a user has network access, all information should be saved to their network drive which is automatically backed up by IT. The C drive is insecure, however users without network access who have to save to the C drive need to implement appropriate security measures to protect any confidential information and ensure appropriate backup.
- 8.3.8. All information should be managed in accordance with supporting information governance policies and procedures.

## 9. Information Classification

9.1. A consistent system for the classification of information within the NHS organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-NHS bodies. NEAS will classify information assets as per the NHS Information Governance guidelines published within the NHS Information Risk Management: Good Practice Guidance to indicate the degree of protection required, dependent on the sensitivity and criticality of the information. Responsibility for defining the classification lies with the identified asset owner. The labelling of assets will be based on the most sensitive aspect of the asset.

### 9.2. General

9.2.1. Data will be classified as:

Data	Security Level	Security Description
Anonymous / no personal details	<u>1</u>	Unclassified
NHS information requiring some degree of protection	<u>2</u>	NHS Protect
Patient identifiable clinical information NHS staff information	<u>3</u>	NHS Confidential

Personal Health Data that includes: <ul style="list-style-type: none"> <li>• Genetic services</li> <li>• Abortion services</li> <li>• Infertility Services</li> <li>• Mental health</li> <li>• Addiction</li> <li>• HIV status</li> </ul>	<u>4</u>	Very sensitive
Such material would cause "grave damage" to national security if publicly available	<u>5</u>	Secret
The highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to <a href="#">national security</a> if publicly available.	<u>6</u>	Top Secret

9.2.2. Level 2 – 4 documents should be kept in locked facilities to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed containers and not unattended at any stage. These documents not in a safe store or transport should be kept out of sight of visitors or others not authorised to view them.

9.2.3. Level 5 and 6 documents will only be made available to a restricted group of staff within the Trust e.g. Chief Executive.

9.2.4. For each classification of information, The Trust will ensure that appropriate handling procedures have been developed to cover processing activities such as:

- Copying.
- Storage.
- Transmission by manual methods such as post.
- Transmission by electronic methods such as Fax or E-mail.
- Transmission by spoken word.

### 9.3. **NHS Confidential**

9.3.1. The endorsement NHS CONFIDENTIAL should also be used to mark all other sensitive information. That is, material the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals.
- Make it more difficult to maintain the operational effectiveness of the organisation.
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations.
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity.
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies.
- Breach statutory restrictions on disclosure of information.

- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.
- 9.3.2. A paper, printout or report etc marked NHS CONFIDENTIAL may also be endorsed with a suitable descriptor indicating the reason for the classification e.g. 'NHS CONFIDENTIAL – PATIENT INFORMATION' or 'NHS CONFIDENTIAL – COMMERCIAL'. A list of the relevant descriptors is included in Table 1 (Appendix 1).
- 9.3.3. Information may be classified NHS CONFIDENTIAL in the light of the circumstances at a particular time. The classification should be kept under review and the information de-classified when the need for this protection no longer applies. NHS use of an equivalent classification for “Restricted” is unnecessary when NHS CONFIDENTIAL is used.
- 9.4. **NHS Protect**
- 9.4.1. In the NHS context, NHS PROTECT should be used with or without descriptors, for information that requires protection below that of NHS CONFIDENTIAL and where care in handling is still necessary. The classification shall be used to mark all other sensitive information such as financial and contractual records.
- 9.4.2. It shall cover information that the disclosure of which is likely to:
- Adversely affect the reputation of NEAS or its officers or cause substantial distress to individuals.
  - Make it more difficult to maintain the operational effectiveness of the organisation.
  - Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or NEAS.
  - Prejudice the investigation, or facilitate the commission of crime or other illegal activity.
  - Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies.
  - Breach statutory restrictions on disclosure of information.
  - Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.
- 9.5. The information asset inventory, classification scheme, information labelling and handling procedures will be subject to regular audit to ensure compliance with this policy. Audit will ensure that:
- The asset inventory is adequate for the needs, is complete and accurate and contains all necessary detail.
  - The classification scheme is suited to business needs and has considered the key measures of confidentiality, integrity and availability.
  - Information labelling provides an accurate representation of the sensitivity of the asset and that labelling is appropriate.

- Information handling procedures adequately reflect Trust needs.

## **10. Access Control**

10.1. Access to business and confidential information must be controlled appropriately. All employees are entitled to use the network and office applications provided by the IT department provided it is applicable to their particular role. Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

10.2. IT will be responsible for administering access to the system and system owners with the responsible for setting the system level access.

### **10.3. User access management**

10.3.1. The Trust has a formal user registration and de-registration procedures which covers networked and non-networked sites, granting and managing access to network directories and systems.

10.3.2. All users of the computer network are required to sign the PC User Account Details section of the PC User Account Pack which will indicate their access needs.

### **10.4. Password control**

10.4.1. Deliberate sharing of system access passwords, is a criminal offence under the Computer Misuse Act 1990. All staff are required to follow good security practices in the selection and use of passwords. This will include:

- Ensuring strong passwords are used i.e. using a minimum 7 digit characters and try to include a numeric or special character.
- Change your password regularly. If you do not change your password after 60 days, the system will lock you out. You will then need to contact the IT Service Desk.
- Not writing down passwords where they can be easily found, i.e. on post-it notes next to their workstation.
- Changing their password immediately if they suspect it has been compromised.
- Ensuring that unattended equipment has appropriate protection. To ensure security, users must either log-off, lock screens or use a password-protected screen saver whichever is most appropriate to their working environment.

### **10.5. Connecting for Health systems controls**

10.5.1. With the implementation of the NHS Care Record Service (NCRS), a number of new systems will be rolled out in the future. These systems will be controlled by a number of different mechanisms and when fully implemented will include:

- Smartcard: Access will be restricted through use of an NHS Smartcard with a passcode, provided by the local Registration Authority.

- Training: Access to the NCRS will only be allowed following appropriate training.
- Legitimate relationships: Staff will only be able to access a patient's record if they are involved in that patient's care.
- Role based access: Access will depend on staff roles / job functions (role-based access). Roles and access privileges will be defined centrally and given locally by people designated to do this within NEAS.
- Sealed envelopes: Patient's will be able hide certain pieces of information from normal view. This will be called a patient's sealed envelope.
- Audit trails: Every time someone accesses a patient's record, a note will be made automatically of who, when and what they did (an audit trail).
- Alerts: Alerts will be triggered automatically both to deter misuse of access privileges and to report any misuse when it occurs e.g. if breach of sealed envelope.

## 10.6. Security of third party access

10.6.1. Access to Trust information processing facilities will be controlled.

10.6.2. Access to facilities will not be allowed until an appropriate risk assessment and resulting security measures have been implemented and an agreement signed defining the terms for access. Assessment of the risks involved in granting third party access will take into account the following areas:

### 1. Type of access required

- Physical access to offices, computer rooms, filing cabinets.
- Logical access to The Trust networks, databases and information systems.

### 2. Reasons for access

- Hardware and software support.
- Partner Organisations or joint ventures.

### 3. Method of remote access if required, i.e. access via NHSnet or direct access via VPN (Virtual Private Network).

10.6.3. Arrangements for third party access to Trust processing facilities will be based on a formal written contract, which contains or refers to all the security requirements to ensure compliance with The Trust policies and standards.

## 11. Monitoring System Access and Use

11.1. An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

11.2. The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of

employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

11.3. Any monitoring will be undertaken in accordance with the above act and the Human Rights Act. The Information Security Lead or deputy will compile monitoring reports and any unusual use of or suspected misuse of resources will be fully investigated. As part of the monitoring process, the Trust business critical systems will also be subject to regular audit by the Internal Audit Department, who will provide reports on the state of the systems security to appropriate managers.

11.4. Monitoring will include all Trust systems. Specific areas that will be monitored will include;

- Failed attempts to access systems.
- Access patterns (log on log off).
- Allocation and activity of privileged accounts.
- Tracking of selected transactions.
- Use of sensitive resources.
- Out of hours activity.
- Inappropriate use of authorised software and IT equipment.
- Any use of un-authorised software and IM&IT equipment.

## **12. Remote Access**

12.1. Remote access occurs when a user logs on to the Trust network from a location where there is no direct access to the Trust's network e.g. a member of staff remotely accessing the network from home.

12.2. Critical business processes rely on easy and reliable access to clinical and corporate information systems.

12.3. Home access to Email, Intranet and Promis is available to users.

12.4. Personal or sensitive data should not be downloaded onto personal equipment under any circumstance.

### **13. Exchanges of Information and Software**

- 13.1. It is imperative that the utmost care is exercised when transferring information, especially information of a confidential nature e.g. staff, patient or service user information. This includes transferring information by telephone (voice and text), email, fax, courier and public mail.
- 13.2. Regular exchanges of information outside of the NHS must be governed by an information sharing protocol using the standard Trust template.
- 13.3. For non-routine exchanges of information, staff must refer to the Caldicott procedure.

### **14. Systems Development and Maintenance**

- 14.1. The Trust must ensure that security requirements are built into systems from the outset. Suitable controls must be in place to manage the purchase or development of new systems and the enhancement of existing systems, to ensure that information security is not compromised.

#### **14.1.1. Security requirements of systems**

Any individual responsible for implementing or modifying systems is responsible, in collaboration with IT for ensuring:

- That statements of business requirements for new systems, or enhancements to existing systems specify the security controls required for that system.
- That all modifications to systems are logged and up to date documentation exists for their systems.
- That vendor supplied software used in systems, is maintained at a level supported by the supplier, if beneficial to the service. Any decision to upgrade must take into account the security of the release.
- That physical or logical access is only provided to suppliers for support purposes when necessary, and must be with management and IT approval.
- That all supplier activity on the system is monitored.
- That copies of data must retain the same levels of security and access controls as the original data.

- 14.1.2. A new system checklist must be completed, in liaison with the Information Governance Team, to ensure all Information Governance aspects of new and modified systems are considered.

- 14.2. The Trust will ensure demands on system capacity are monitored and projections of future capacity requirements are made to ensure that it has adequate processing and storage facilities available. The utilisation of key system resources, such as file servers, e-mail servers and business critical systems will be monitored so that additional capacity can be brought on-line when required.

## **15. Incident and Risks**

- 15.1. The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.
- 15.2. All breaches of information security, actual or suspected, shall be recorded, reported to and investigated by the Information Security Lead(s) via the standard procedures for risk and incident reporting.
- 15.3. Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of a risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.
- 15.4. Reporting of risks and incidents is important to ensure that appropriate action is taken so that risks / incidents do not reoccur and to learn from them. No constructive action can be taken if the organisation is not notified when things go wrong or there is a near miss.
- 15.5. The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

## **16. Disaster Recovery Plan**

- 16.1. Full disaster recovery plans must exist that allow critical systems to be maintained and to restore critical systems in the event of a major disruption to systems e.g. through a disaster or security failure. This supports the wider NEAS business continuity planning.
- 16.2. Plans for all IT Systems and Network & Telephony facilities will be produced by the IT Department. There is currently a programme in place to ensure progress is made. The responsibility to co-ordinate any table top exercise will be a combination of the System Owner and the IT Technical Lead.

## **17. Consultation, Approval and Ratification Process**

- 17.1.1. This document has been produced by the author on behalf on the IGWG. This group was consulted upon and their comments added to the document as appropriate.
- 17.2. **Approval and ratification**
  - 17.2.1. The Trust Policy Sub Group is the committee with the authority for the approval and ratification of this document.

17.2.2. The IGWG has carried out a full and proper consultation and has considered the content of the document in terms of current best practice, guidelines, legislation and mandatory and statutory requirements, in considering the document for approval the committee also took into account the results of the recommendations of the EIA.

## **18. Review and Revision Arrangements**

18.1. The document will be reviewed at least annually or when appropriate after changes in legislation or guidance. The document owner will be responsible for this review.

## **19. Dissemination and Implementation**

### **19.1. Dissemination**

19.1.1. This policy is available for all staff to access via the Trust Quality System. Staff without computer network access should contact their line manager for information on how to access policies.

19.1.2. All staff will be notified of new or revised documents via internal communications systems.

19.1.3. This document will also be included in the Publication Scheme for NEAS in compliance with the FOI Act 2000.

### **19.2. Implementation**

19.2.1. This policy will be implemented in the following ways:

- Regular communications to staff on new policies and procedures through Information Governance circulars.
- Regular audit of IG processes undertaken in line with policies and procedures in key areas i.e. records management, confidentiality, information security, FOI and data quality.
- Monitoring through the Information Governance Toolkit (IGT).

### **19.3. Training**

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

19.3.2. Broad IG training will be included in the Trust induction programme. Additional training can be requested at the discretion of a manager, or by an individual wanting personal development along with mandatory yearly update training.

19.3.3. Further guidance and information relating to data protection issues will be distributed periodically via various media including the intranet site, 'The Pulse' (monthly service journal) and via email.

## **20. Document Control Including Archiving Arrangements**

### **20.1. Register / library of procedural documents**

All documents shall be held within the Trust Quality System and will be managed in line with quality standards.

## 20.2. **Archiving arrangement**

Archiving of documents will be in line with the Records Management Policy.

## 21. **Monitoring Compliance With and the Effectiveness of Procedural Documents**

### 21.1. **Process for monitoring compliance**

21.1.1. All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for data protection.

21.1.2. Failure to follow this policy and related IG policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

21.1.3. Monitoring staff compliance through:

- Verifying that, where appropriate, agreement to disclosure decisions are recorded.
- Obtaining patient feedback of the process, e.g.:
  - Did they understand when and to whom their information would be disclosed?
  - Did they understand the choices available to them regarding disclosure?
  - Did they have the opportunity to ask questions and have them answered?
  - Did they understand that withholding of consent does not affect the way they are handled by staff but may reduce the number of treatment options available to them?
  - Did they feel under pressure to agree to disclosure?
- Evaluating whether staff understand disclosure issues and their responsibility for obtaining consent.
- Evaluate how staff handled questions about disclosure, and in particular review cases where:
  - Patients have declined to agree to disclosure.
  - Patients have changed their disclosure decision during the care episode.
  - A senior healthcare professional has overridden a non-disclosure decision.

### 21.2. **Standards and Key Performance Indicators**

There are a number of national standards and requirements relating to IG.

#### 21.2.1. **IG Toolkit**

The connecting for Health IGT is a framework for implementing the IG agenda and consists of a series of requirements against which an organisation's current and planned attainment levels can be monitored. The Trust is required to complete a self assessment by 31st March each year, the results which will contribute to the assessment undertaken by the Healthcare Commission.

### 21.2.2. Standards for Better Healthcare

- The Department of Health's standards for better health include 24 core standards that all NHS healthcare providers in England should achieve, and 13 developmental standards that they should be working towards achieving.
- Core standard 13 requires that health care organisations have systems in place to ensure that:
  - Staff treat patients, their relatives and carers with dignity and respect;
  - Appropriate consent is obtained when required for all contracts with patients and for the use of any patient confidential information; and
  - Staff treat patient information confidentially, except where authorised by legislation to the contrary.

### 21.2.3. NHS Litigation Authority

- The NHSLA Risk Management Standard for Ambulance Trusts applies to all Ambulance Trusts are designed to address organisational, clinical, and non-clinical / health and safety risks.
- Parts of the Clinical Care standard are of relevance to IG, including patient / service user identification and quality of written and electronic clinical records.

## 22. References

- Department of Health NHS IG Guidance on Legal and Professional Obligations.
- NHS Connecting for Health IG Toolkit <https://www.igt.connectingforhealth.nhs.uk/>

## Appendix A: Classification of NHS Information - Marking Guidance for NHS

### Organisations

**NHS CONFIDENTIAL** - appropriate to paper and electronic documents and files containing person-identifiable **clinical** or NHS **staff** information and **other sensitive** information.

**NHS PROTECT** – Discretionary marking that may be used for information classified below NHS Confidential but requiring care in handling. Descriptors may also be used as required.

**Table 1 – Descriptors that may be used with “NHS CONFIDENTIAL” or “NHS PROTECT” marking**

Category	Definition
<b>Appointments</b>	Concerning actual or potential appointments not yet announced.
<b>Barred</b>	Where <ul style="list-style-type: none"> <li>• there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or</li> <li>• disclosure would constitute a contempt of Court (information the subject of a court order).</li> </ul>
<b>Board</b>	Documents for consideration by an organisation’s Board of Directors, initially, in private. (Note: This category is not appropriate to a document that could be categorised in some other way.)
<b>Commercial</b>	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.
<b>Contracts</b>	Concerning tenders under consideration and the terms of tenders accepted.
<b>For Publication</b>	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date.
<b>Management</b>	Concerning policy and planning affecting the interests of groups of staff. (Note: Likely to be exempt only in respect of some health and safety issues.)
<b>Patient Information</b>	Concerning identifiable information about patients
<b>Personal</b>	Concerning matters personal to the sender and / or recipient.
<b>Policy</b>	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published).
<b>Proceedings</b>	The information is (or may become) the subject of, or concerned in a legal action or investigation.
<b>Staff</b>	Concerning identifiable information about staff

**Table 2 - Freedom of Information Act Exemptions**

<b>Category</b>	<b>Possible Exemption [section(s) of the FOI Act]</b>
<b>Appointments</b>	S 40 Personal information (may be subject to a public interest test)
<b>Barred</b>	S 44 Legal prohibitions on disclosure
<b>Board</b>	
<b>Commercial</b>	S 43 Commercial interests (subject to a public interest test)
<b>Contracts</b>	S 43 Commercial interests (public interest test)
<b>For Publication</b>	S 22 For future publication (public interest test)
<b>Management</b>	S 38 Endanger health and safety (public interest test)
<b>Personal</b>	S 40 Personal Information (may be subject to public interest test)
<b>Policy</b>	S 22 For future publication (public interest test)
<b>Proceedings</b>	S 30 Investigations and proceedings S 31 Law enforcement