NHS
North Staffordshire
Combined Healthcare
NHS Trust

Doc level: Trustwide
Code ref: 7.03

Information Security & Data Protection Policy

Lead executive	Director of Finance
Authors details	Information Security Manager

Type of document	Policy
Target audience	All Trust staff
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet its legal obligations under Data Protection & Information Security legislation it sets standard requirements for the management of information and to support Information Governance

Approving meeting	QUALITY COMMITTEE TRUST BOARD	Meeting date	27 SEPTEMBER 2018 25 OCTOBER 12018
Ratification date	25TH OCTOBER 2018	Review date	31 OCTOBER 2021

Trust documents to be read in conjunction with	
Document code	Document name
3.01	Disciplinary Procedure
4.18a & b	Risk Management Policy and Strategy
7.01	Confidentiality of Employee and Patient Records
7.02	Subject Access Request Policy
7.07	Records Management Policy
7.14	Safe Haven Policy
7.19	Mobile Information Handling Policy
7.22	Registration Authority Policy

Document change history		Version	Date
What is different?	– This policy has been revised in line with legislation changes under Data Protection.		
Appendices / electronic forms	–		
What is the impact of change?	– Making all staff aware of changes in legislation; – Ensuring that the Trust is compliant with its legal requirements under Data Protection and Information Governance – The policy sets the strategic and operational requirements to support Information Governance and includes legislative and NHS mandates.		

Training requirements	Training relating to the areas this policy cover is addressed in the mandatory Data Security Awareness training that all staff have to complete annually

Document consultation	
Directorates	
Corporate services	
External agencies	

Financial resource implications	None

External references
1. Data Protection Bill 2. General Data Protection Regulations (GDPR)

Monitoring compliance with the processes outlined within this document	This policy will be monitored and updated accordingly by the Information Governance Steering Group

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favorably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
– **Religion and/or Belief** (includes those with religion and /or belief and those with none)		
– **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other	No	

groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)		
If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.		
Enter details here if applicable		
If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?		
Enter details here if applicable		
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No	
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A	
Enter details here if applicable		
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

CONTENTS

The Information Security Documents (ISDs) at the end of this policy relate to measures that should be taken to ensure that manual and computerised information and data is protected.

ISD A - Data Protection Act and Caldicott Principles (*page 15*)	What you should know about the DPA and Caldicott Principles
ISD B – Physical Site Security Procedures (*page 18*)	The physical locating, maintenance and disposal of computer hardware
ISD C – Computer Access Procedures (*page 19*)	User Registration, Log-on Procedures, Password Control, Access Levels, Automated Password Management, and Leavers.
ISD D – Data Housekeeping Procedures (*page 21*)	Saving, Deleting and Backing Up files
ISD E – Email Use (*page 22*)	Guidelines for the safe and ethical use of electronic mail. *(see also ISD J for Secure Email Guidance – page 23)*
ISD F – Internet Access (*page 25*)	Guidelines for the use of the Internet
ISD G – Incident Reporting (*page 26*)	Information Security Risk Management & Incident Reporting Procedure
ISD H - Virus Control (*page 27*)	Virus protection software. Spam, Chain Mail, Jokes and Unsolicited Messages
ISD I – Smartcards (*page 28*)	NCRS Acceptable Use, Terms & Conditions
ISD J - Transmission of PID (*page 29*)	Secure Email Guidance and eFax
ISD K – Software Licensing (*page 30*)	Installation and Responsibilities
ISD L – Encryption of Mobile	All NHS mobile computing devices to

Devices (*page 31*)	be encrypted
ISD M – Social Media & Social Networks - Acceptable Use Policy (*page 32*)	Guidance on the use of social networking sites.

1. Policy Statement

1.1. North Staffordshire Combined Healthcare NHS Trust is committed to ensuring that all person-identifiable information/data that is received, stored, processed, transmitted, whether by manual, computerised or spoken methods is done so in a secure environment. This Policy intends to set Trust-wide standards for safeguarding manual and computerised information/data through the use of technical developments and organisational management procedures.

1.2. The Information Security & Data Protection Policy has been written in order to set standard requirements for the management of information, and to support Information Governance at North Staffordshire Combined Healthcare NHS Trust (hereafter referred to as the Trust). The NHS Executive and UK Judiciary mandate NHS Trusts to set strategic and operational Policy standards for the secure and appropriate management of information. These standards are monitored by the Information Governance Toolkit.

1.3. This Policy sets the strategic and operational requirements to support Information Governance, and includes legislative and NHS mandates, which directly impact on the Policy. The Policy refers to **Information Security Documents (ISDs)**. ISDs are intended to be a user-friendly vehicle for implementing the strategic and operational mandates into practical instruction for Trust staff.

1.4. This Policy is set within the NHS's strategic approach to Information Governance, addressing issues of patient confidentiality, set within the context of the eight principles of the Data Protection Act, The Freedom of Information Act 2000 and the recommendations of the Caldicott Principles and Review of 2013.

2. Scope

2.1. Data stored on computer and manual systems is a valuable asset to the Trust. National safeguards surrounding personal data have undergone significant change over recent years.

2.2. Furthermore, the Caldicott Report and Review of 2013, and its recommendations, will be implemented in parallel with many issues contained within the Data Protection Act.

2.3. It is important to note that personal information relates to more than simply patient information. Employee, financial information, occupational health and commissioning information in relation to the purchase of goods and services are of equal importance.

2.4. The term 'person identifiable' is referred to throughout this Policy and means information of a personal nature, which could reasonably identify someone. In terms of a patient, the common identifiers are for example name, age, gender and address. In relation to personnel, volunteer, contractor and finance information, identifiers may differ but should still be deemed confidential.

2.5. The scope of this Policy applies to all permanent and/or contracted staff employed by the Trust.

2.6. The Data Protection Act provides a wide definition as:

- Obtaining, recording or holding the information;

- Carrying out any operation or set of operations on the information;
- Organising, adapting and amending the information;
- Retrieval, consultation and use of the information.

2.7. Any breaches of adherence to this Policy and the corresponding ISDs, will be subject to the existing Trust Disciplinary Policy 3.01.

2.8. This Policy will be referred to when dealing with other agencies in order to give clear guidance on this Trust's approach to confidentiality and data security. This Policy does not represent the policies, procedures or guidelines of other agencies.

2.9. Key issues addressed by this policy

Confidentiality	Information is required to be 'fit for the purpose', access confined to those with specified authority to hear, view, process and store information.
Integrity	Systems are operating correctly according to their specification and in the way users believe them to be operating.
Availability	Information is delivered to the right person when it is needed.

3. Duties

General Trust Responsibilities

3.1. The Trust is responsible for ensuring implementation, education and training in respect of this policy. An overview of data protection and security is given during the organisation induction days for new starters.

Management Responsibilities

3.2. Trust managers are responsible for:

- Monitoring and reporting on the state of IM&T security within the organisation.
- Monitoring for actual or potential data security breaches. A breach in security shall be properly reported immediately via the Trusts 'Safeguard' Incident Reporting System; investigated and, where appropriate, disciplinary action be taken.
- Providing reports on breaches of information security to the Trust's Risk Management Committee and where appropriate to Operational Board in accordance with the Trust's Risk Management Policy 4.18a and Strategy 4.18b.
- Ensuring that the Information Security & Data Protection Policy is implemented throughout the Trust.
- Developing and enforcing detailed procedures to maintain security.
- Ensuring compliance with relevant legislation.
- Ensuring that the Trust's employees are aware of their responsibilities and accountability for data security and confidentiality.

3.3. Management shall ensure that individuals who operate any computer equipment including PDAs, Remote Access Tokens, stand-alone PCs, laptops, tablets or whose equipment is linked to the main network systems, will be responsible for:

- Identifying all the data for which they are responsible.
- Ensuring compliance with security controls.

- Ensuring compliance with Data Protection and other legislation where appropriate.
- Periodically reviewing these responsibilities.

3.4. To uphold the principles of the Data Protection Act, the General Data Protection Regulation (GDPR), the Freedom of Information Act, and the Caldicott Report and Review of 2013, line managers are responsible for ensuring that their staff clearly understand the following:

- The Trust's Information Security & Data Protection Policy and its procedures for disclosure of information including specific reference to the spoken word (*Confidentiality of Employee and Patient Records Policy 7.01*).
- The legal obligations of staff (Data Protection Act, GDPR and Freedom of Information Act).
- The extent of staff authorisation to access personal information. Access should be based on the user's employment position and requirement under that post to access information.
- Consequences of breaches of this Policy.
- Retention periods for documents relevant to each Department/Directorate via the Trust's Records Management Policy 7.07, which includes reference to the safe destruction of documents.

3.5. New software, which has not been properly developed and/or properly tested, is a threat to the security of existing data. All software and hardware procurements shall take account of the Trusts security requirements. This shall specifically include the procedures and actions for handing over and testing new software. Contravention of the recommendations may be considered a disciplinary offence

3.6. Advice regarding the purchase of new software and hardware should be obtained by contacting SSHIS. In addition, specifications and purchasing advice for hardware, printers and scanners is available on the Trust Intranet. The order and receipt of goods will be authorised and processed by SSHIS. Procurement shall take account of the need for compatibility to support the installation's contingency and recovery arrangements. Orders for new IT equipment will be checked by SSHIS for a technical signature before purchase.

3.7. **Transfer of Equipment** - If equipment is transferred to other areas or individuals, the IT Service Desk must be informed. This procedure ensures that there is an accurate audit database.

3.8. **Notification of Staff Changes** - It is the responsibility of line managers to notify the SSHIS Service of changes in staff circumstances that may affect access to systems. These include Job Title, work location, membership of Access Control Lists and Distribution Groups, Maternity/Sick leave (*see also ISD E – Email Guidelines / Long-term absence).*

3.9. **The Caldicott Guardian** will authorise access on key issues such as sharing information and the protection and use of patient-identifiable information. The Caldicott Guardian will also advise the Trust Board on progress and issues as they arise.

Staff Responsibilities

3.10. The Data Protection Act, GDPR and the seven key principles of the Caldicott recommendations, place clear responsibilities on data users, controllers and processors of information/data. Once staff have received basic education relating to this Policy they are expected to adhere to it as they would other Trust policies.

3.11. All staff that have access to person-identifiable information have a responsibility for the security and confidentiality of such information in accordance with this and other Trust Policies and Procedures.

3.12. All staff have a responsibility for reporting information security incidents via the Trusts Safeguard Incident Reporting System.

3.13. No member of staff is permitted to save files that contain offensive material. To do so may constitute a serious breach of Trust security and could result in dismissal and/or criminal prosecution. *(See ISD E)* The Trust is the final arbiter on what is or is not offensive material.

Education, Training and Awareness

3.14. Data Security Awareness Training will be included as part of the Trust induction programme and mandated training.

3.15. It is the responsibility of line management to ensure that all new staff attend the induction programme and complete the Data Security Awareness eLearning.

3.16. To ensure the quality of data is maintained, it is the responsibility of managers to ensure that individuals attend systems training at the appropriate time, e.g. at the commencement of employment, job change or system change.

3.17. Prior to operating any clinical systems all potential users, including temporary/agency staff, must receive system training according to the access level required.

3.18. Managers must use their discretion in assessing an individual's competence and aptitude before allowing an employee to commence work, e.g. testing at recruitment stage.

4. Framework

4.1. **Information Governance**:

The Department of Health has promoted the concept of information governance through the introduction of the Information Governance Toolkit. The toolkit details legal and policy requirements in respect confidentiality, data protection, freedom of information, records management, information quality and information security. The Department of Health requires NHS organisations to complete the toolkit annually, and uses it to monitor compliance.

4.2. **Data Protection Act – Key Principles** (*see ISD A*)

1 Personal data shall be processed fairly and lawfully.
2. Personal data is obtained only for one or more specified lawful purposes.
3. Data shall be adequate, relevant and not excessive.
4. Data shall be accurate and up to date.
5. Data shall not be kept for longer than is necessary.

6. Data shall be processed in accordance with the rights of data subjects in mind.
7. Safeguards against unauthorised or unlawful processing of personal data and safeguards against accidental loss or destruction of, or damage to, personal data.
8. Secure transfer of data outside the European Union.

4.3. The Act places increased responsibilities on organisations to further recognise and respect the individual's right to privacy. The Data Protection Act includes both manual and computerised records that are be dealt with by one form of legislation. In addition staff are under a common law obligation to preserve the confidentiality of this information. The Data Protection Act and GDPR relate to any structured, relevant filing system that identifies a living individual. In respect of the deceased, the Access to Health Records Act 1990 applies.

4.4. In 1997 a report was published entitled the Caldicott Committee Report on the Review of Patient Identifiable Information. The report found that the issues of patient confidentiality and the security measures in place across the NHS lacked national consistency. As a result of the Caldicott Report and the subsequent Review of 2013, seven key principles were provided as a guide for the NHS.

4.5. **Caldicott Key Principles**:

1 Justify the purpose(s) for collecting and sharing patient information.
2. Do not use patient-identifiable information unless it is absolutely necessary.
3 Use the minimum necessary patient-identifiable information.
4. Access should be on a need to know basis.
5. Everyone should be aware of his or her responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality

5. Implementation and Monitoring

The principles of the Information Security & Data Protection Policy will reduce from 8 to 6 following the implementation of the GDPR in May 2018. The policy also needs to keep pace with changes in IM&T systems and developments and changes in manual data handling, and will therefore be updated in between formal review as required.

6. References

Data Protection Act	Freedom of Information Act
Department of Health – Information Security Management NHS Code of Practice	Records Management and the NHS Code of Practice Parts 1 & 2
Protecting and Using Patient Information: A Manual for Caldicott Guardians	One Staffordshire Protocol
The NHS Confidentiality Code of Practice	Computer Misuse Act 1990
The NHSnet Acceptable Use Policy	The Care Record Guarantee

	January 2011 (Smartcards)
Copyright, Patents & Designs Act 1988	The Communications Act 2003
The General Data Protection Regulation (GDPR)	

7. Associated Policy and Procedural Documentation

Policy No 3.01 - Disciplinary Procedure

Policy No 4.18a – Risk Management Policy and Strategy (4.18b)

Policy No 7.01 - Confidentiality of Employee and Patient Records

Policy No 7.02 - Access to Health and Employee Records

Policy 7.07 – Records Management Policy

Policy 7.14 – Safe Haven Policy

Policy 7.19 – Mobile Information Handling Policy

Policy 7.22 – Registration Authority Policy (for Smartcards)

Appendix 1 - North Staffordshire Combined Healthcare Trust Data Classification and Access Control Protocol

1. Information Services Responsibility—All employees who come into contact with sensitive North Staffs Combined Healthcare Trust (NSCHT) internal information are expected to familiarise themselves with this data classification policy and to consistently use these ideas in their daily NSCHT activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, Trust employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for the trust in classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these sensitivity classifications.

2. Addresses Major Risks - The IT data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect NSCHT information from unauthorised disclosure, use, modification, and deletion.

3. Applicable Information - This data classification policy is applicable to all electronic information for which the Trust is the custodian.

PROCEDURES

1. Access Control

1.1 Need to Know—each of the policy requirements set forth in this document is based on the concept of the need to know. If an employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business or service need for the information.

1.2 System Access Controls—the proper controls will be in place to authenticate the identity of users and to validate each user's authorisation before allowing the user to access information or services on the system. Data used for authentication will be protected from unauthorised access. Controls will be in place to ensure that only personnel with the proper authorisation and a need to know are granted access to NSCHT systems and their resources. Remote access will be controlled through identification and authentication mechanisms.

1.3 Access Granting Decisions—access to NSCHT sensitive information must be provided only after the written authorisation of the Data Owner has been obtained. Access requests will be presented to the data owner as per the Subject Access Request Policy No. 7.03. Custodians of the information must refer all requests for access to the relevant Owners or their delegates. Special needs for other access privileges will be dealt with on a request-by-request basis.

2. Information Classification

2.1 Owners and Production Information—all electronic information managed by the Trust must have an Information Asset Owner. Production information is information routinely used to accomplish business objectives. Owners should be Director level and responsible for

assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. There are designated members of the NSCHT management team who act on their behalf, and who supervise the ways in which certain types of information are used and protected.

2.2 RESTRICTED—this classification applies to the most sensitive business information that is intended for use strictly within NSCHT. Its unauthorised disclosure could seriously and adversely impact NSCHT, its service users, its business partners, and its suppliers.

2.3 CONFIDENTIAL—this classification applies to less-sensitive business information that is intended for use within NSCHT. Its unauthorised disclosure could adversely impact NSCHT or its service users, suppliers, business partners, or employees.

2.4 PUBLIC—this classification applies to information which has been approved by NSCHT management for release to the public. By definition, there is no such thing as unauthorised disclosure of this information and it may be disseminated without potential harm.

2.5 Owners and Access Decisions—Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. The Trust must take steps to ensure that appropriate controls are utilised in the storage, handling, distribution, and regular usage of electronic information.

3. Object Re-use and Disposal

Storage media containing sensitive (i.e. restricted or confidential) information will be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the Chief Information Officer.

4. Physical Security

4.1 Data Centre Access—Access to the data centre must be physically restricted in a reasonable and appropriate manner.

4.2 Facility Access–All network equipment (routers, switches, etc.) and servers located in the corporate office and in all facilities must be secured when no NSCHT personnel, or authorised contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorised personnel.

5. Special Considerations for Restricted Information

If restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to data access control safeguards approved by the Information Governance Team and Corporate senior management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

5.1 Data Encryption Software—NSCHT employees and vendors must not install encryption software to encrypt files or folders without the express written consent of Information Security.

6. Information Transfer

6.1 Transmission Over Networks—If NSCHT Restricted data is to be transmitted over any external communication network, it must be sent only in encrypted form. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual public network or similar software as approved by the Information Security Team.

6.2 Transfer To Another Computer—before any restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

7. Software Security

7.1 Secure Storage of object and source code—Object and source code for system software will be securely stored when not in use by the developer. Developers must not have access to modify program files that actually run in production. Changes made by developers must be implemented into production by independent technical staff. Unless access is routed through an application interface, no developer will have more than read access to production data. Furthermore, any changes to production applications must follow the change management process.

7.2 Testing—Developers must at least perform unit testing. Final testing must be performed by the Clinical Systems Team or the target user population.

7.3 Backups—Sensitive data will be backed up regularly, and the backup media will be stored in a secure environment.

8. Key Management

8.1 Protection of Keys—Public and private keys will be protected against unauthorised modification and substitution.

8.2 Procedures—Procedures will be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

8.3 Safeguarding of Keys—Procedures will be in place to safeguard all cryptographic material, including certificates. SSHIS must be given copies of keys for safekeeping.

INFORMATION SECURITY DOCUMENT A

The Data Protection Act, GDPR and Caldicott Review

Data Protection Act

The Data Protection Act seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.

The DPA gives individuals certain rights regarding information held about them. It places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual.

The eight principles of the Data Protection Act

Anyone processing personal information must comply with eight enforceable principles of good information handling practice.

These say that personal information must be:

1. **fairly and lawfully processed**
2. **processed for limited purposes**
3. **adequate, relevant and not excessive**
4. **accurate and up to date**
5. **not kept longer than necessary**
6. **processed in accordance with the individual's rights**
7. **secure**
8. **not transferred to countries outside European Economic area unless country has adequate protection for the individual**

The six conditions

At least one of the following conditions must be met for personal information to be considered fairly processed:

1. the individual has consented to the processing
2. processing is necessary for the performance of a contract with the individual
3. processing is required under a legal obligation (other than one imposed by the contract)
4. processing is necessary to protect the vital interests of the individual
5. processing is necessary to carry out public functions, e.g. administration of justice
6. processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual)

Sensitive data

Specific provision is made under the Act for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

For personal information to be considered fairly processed, at least one of several extra conditions must be met. These include:

- Having the explicit consent of the individual
- Being required by law to process the information for employment purposes
- Needing to process the information in order to protect the vital interests of the individual or another person
- Dealing with the administration of justice or legal proceedings

Rights under the Act

1. The right to subject access
This allows people to find out what information is held about them on computer and within some manual records.

2. The right to prevent processing
Anyone can ask a data controller not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else.

3. The right to prevent processing for direct marketing
Anyone can ask a data controller not to process information relating to him or her for direct marketing purposes.

4. Rights in relation to automated decision-taking
Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.

5. The right to compensation
An individual can claim compensation from a data controller for damage and distress caused by any breach of the act. Compensation for distress alone can only be claimed in limited circumstances.

6. The right to rectification, blocking, erasure and destruction
Individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

7. The right to ask the ICO to assess whether the Act has been contravened
If someone believes their personal information has not been processed in accordance with the DPA, they can ask the ICO to make an assessment. If the Act is found to have been breached and the matter cannot be settled informally, then an enforcement notice may be served on the data controller in question.

The General Data Protection Regulation (GDPR)

The GDPR is European Union (EU) legislation that becomes directly applicable in the UK from 25th May 2018. The GDPR strengthens the controls that organisations are required to have in place over the processing of personal data.

Headline impacts are:

- Appointment of Data Protection Officer (DPO) mandatory for all public authorities
- Organisations obliged to demonstrate that they comply with the new law (the concept of 'accountability').
- Significantly increased penalties possible for any breach of the Regulation – not just data breaches.
- Legal requirement for security breach notification.
- Removal of charges, in most cases, for providing copies of records to patients or staff who request them.
- Requirement to keep records of data processing activities.
- Data Protection Impact Assessment required for high risk processing (which includes the large-scale processing of health-related personal data).
- Data protection issues must be addressed in all information processes.
- Specific requirements for transparency and fair processing.
- Tighter rules where consent is the basis for processing.

Legal requirements require organisations to take specified actions, and have evidence to demonstrate that they have done so. Much of this is covered by the IG Toolkit.

Additional information is available on the Information Commissioner's Website **http://ico.org.uk**

Caldicott Review

The Caldicott review was commissioned by the Chief Medical Officer to investigate the ways in which patient information is used in the NHS. The Caldicott committee made a number of recommendations aimed at improving the way the NHS handles and protects patient information.

When using Person Identifiable Data you must:

1. **Justify the purpose**
2. **Use only when absolutely necessary**
3. **Use the minimum information required**
4. **Access only on a strict need-to-know basis**
5. **Understand YOUR responsibilities**
6. **Understand and comply with the law (Data Protection Act)**
7. **The duty to share information can be as important as the duty to protect patient confidentiality**

Following the review in 2003 the seventh principle was added regarding sharing information with the comment:

"Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies".

Additional Information

Additional guidance on the Data Protection Act and Caldicott Review is available at **http://ico.org.uk**

INFORMATION SECURITY DOCUMENT B
PHYSICAL SITE SECURITY PROCEDURES

IT Equipment

- IT equipment should be situated away from areas where the general public could view the screen.
- Users must not leave their terminal or PC unattended with confidential information on display.

Clear Desk and Screen

- Computers should be locked when they are not in use to prevent others using your logon whilst you are out of the office.
- All confidential papers/documents should be stored in suitable lockable drawers or cabinets when not in use and at the end of the day.
- At the end of meetings all documents should be cleared from tables before exiting the room.
- Reception areas should be kept as clear as possible to avoid medical or personal documents being within reach/sight of any visitors to the Trust and any visitor, appointment or message books should be stored in a locked area when not in use.

Off-Site Equipment

- Portable electronic equipment must be kept in the possession of a Trust employee during transportation. If such equipment is lost or stolen, the matter must be reported to your line manager and the SSHIS Service Desk immediately.
- Portable electronic equipment must have encrypted protection against unauthorised use. Passwords for example on boot-up (when a computer is switched on), should be incorporated.
- Portable computers must have Trust approved anti-virus software installed.

Equipment Disposal

The Trust and its employees/contractors have a responsibility to ensure responsible final disposal of all Waste Electronic and Electrical Equipment under several EU Directives including the Landfill Directive, The European Waste Electronic & Electrical Equipment (WEEE) Directive COM (2000) 347 and the Reduction of Hazardous Substances Directive.

Register of New / Existing Electronic Equipment

Because of risks associated with inappropriate disposal of electronic equipment, the Trust requires items such as desktop PCs, laptops, Personal Digital Assistants etc. with data holding capacity to be recorded in an appropriate Asset Register when purchased. This is primarily to record ownership and any transfer thereof, of specifically that equipment which has the capacity to hold:

- Data which might be subject to Data Protection legislation
- Data which might be of a confidential or sensitive nature or
- Software applications where the Trust holds the individual or site license.

Reuse of Surplus Equipment within the Trust

Departments should follow a general policy of internal cascading of any surplus equipment within their own area.

Responsible Disposal for Recycling

If no use can be found within the Trust for unwanted equipment, or it is no longer functioning, it should be disposed of by contacting the SSHIS Service Desk, who will make all necessary arrangements. Simply by deleting files from the disk, or formatting a disk does not ensure that the information has been permanently destroyed.

INFORMATION SECURITY DOCUMENT C

COMPUTER ACCESS PROCEDURES

Computer System Access Control

Line management must ensure that only authorised staff i.e. appropriate to their role, have access to hardware, software and data. Access authorisation should be regularly reviewed, particularly when staff roles and responsibilities change.

Physical Access Controls

All staff must be aware that physical security measures must be taken to restrict access to certain work areas of the Trust. Critical installations should be protected, at the minimum, by lock and key with only authorised staff permitted access. Staff must ensure that they consider whether theft, damage or malicious use of information may occur.

Prevention of Misuse

Any use of IM&T facilities for non-business or unauthorised uses without management approval will be regarded as inappropriate usage.

The Computer Misuse Act 1990 introduced three criminal offences. Staff must remember that the following offences can be enforced in a court of law:

- Unauthorised access
- Unauthorised access with intent to commit further serious offence
- Unauthorised modification of computer material

Obtaining a Network Account

It is NHS policy that all staff should have access to Electronic Mail. To use email you require a network account. You also require an account to access applications such as Lorenzo, ESR etc.

A potential new user and their line manager should complete an ***Application for Network Account Form***, available on the Intranet

Closing a Network Account

Managers should notify the SSHIS Service Desk of all leavers so that their network account can be disabled. Emails are retained on a leavers Outlook account for 12 months and then permanently deleted.

Data and Information Access

- Users will only be granted access to data and information that it is required as part of their job. Access is therefore granted on a 'need to know' basis.
- Staff must not access computer systems or data unless they have authority to do so. Access to files which are not in the course of the employee's duty will be considered a serious disciplinary offence, for example – accessing a friend or relatives manual or electronic file. .

Passwords

For access to the network the current policy settings enforce password changes every 60 days. Passwords must be a minimum of 6 characters and should contain a mixture of letters, upper case and lower, characters (such as £) and numbers. The previous 12 passwords cannot be reused. You should register on 'Fastpass' at the earliest opportunity to set up a password recovery link for instances of forgotten passwords.

Passwords should not be documented, listed or stored in any way. If you feel that your password is not secure, you must change it immediately and notify your concerns about security to your line manager.

There are absolutely no circumstances where it is justifiable to share your password with anyone. If another person requires

and is entitled to network access, they will have their own login identity issued. Always remember that all actions carried out on a computer are recorded and attributed to the user currently logged on at the workstation. Please be aware that disciplinary action will be taken against any member of staff who shares their password.

Training

It is the responsibility of line managers to ensure that all staff receives appropriate training in the use of the IT systems for which they have been given access.

Remote Access

NHS Security Standards and IGT requirements mandate that all remote access by users and suppliers should be subject to strong authentication before access is given to this Trusts computer networks. The Trust enforces two factor authentication for all users, and where appropriate suppliers, and this is managed and operated by the SSHIS.

Third Party Access

Third parties will not be given access to systems or networks unless the Trust/persons in question have formal authorisation to do so. All non-NHS companies will be required to sign security and confidentiality agreements with the Trust.

Third parties found accessing elements of the system that they are not authorised to, will be deemed a security breach and will be denied access immediately. An investigation will take place to decide the outcome.

The NHSnet Code of Connection and this policy will be deemed to be breached if the use of modem connections on the Trust's network is permitted without approval from SSHIS. Modem connections from stand-alone computers are also not permitted. This applies particularly to connections to the Internet.

INFORMATION SECURITY DOCUMENT D

HOUSEKEEPING PROCEDURES

Use of the Storage Area Network

The Storage Area Network (SAN) provides a number of alternative locations for storing data. Where you choose to store files will be dictated by local working practices but in general, data that is accessed by more than one person is stored on shared network drives (X etc.) and data that is for your individual use is stored on your individual drive (U).

Staff are responsible for ensuring that any files they create are regularly reviewed and files that are no longer required are deleted.

Backing Up of Data

You are only required to back-up the data that you personally produce. Systems data (e.g. Lorenzo) is automatically backed-up. Although personal files stored on the Storage Area Network are backed-up by the IT Service, this is for emergency recovery purposes only and should not be viewed as a failsafe for your data.

Media Storage

All media that contains confidential information must be kept in a secure environment. All removable media must be locked away in a secure storage environment at the end of the working day.

Disposal of Confidential Paper Waste

Confidential paper waste must be disposed of separately to 'standard' waste. Confidential waste may contain any of the following:

- Persons name
- Persons address
- Persons postcode
- Any personal identifiers, e.g. Unit Number, Personnel Number
- Commercial in Confidence e.g. budgets, contracting information

All confidential waste must be stored securely in an office, ward, clinic etc. until it is disposed of. It must not be left lying around on desks or in public area The Trust may be at risk if confidential waste is found by people that should not have access to it.

Confidential waste must be placed in appropriately marked repository bins, bags or sacks. All confidential waste must be disposed of (incinerated or shredded) under supervision.

INFORMATION SECURITY DOCUMENT E

EMAIL USE

Email is provided to staff as a business tool, but because of its potential for misuse and abuse it is necessary to have in place a range of rules / guidelines to promote acceptable use for the protection of both the user and the Trust. These rules and guidelines are based on current legislation and common-sense principles. Their purpose is:

- To ensure that email is used effectively, an understanding of how it works and of good practice and etiquette that applies to its use
- To protect the users and the Trust from the risk of legal liability as a result of email abuse.
- To protect and maintain the quality of Trust information against threats via external intrusion.

Long-Term Absence

If a staff member is on long-term absence (more than four weeks), their line manager should with the help of the IT Service, redirect the account to someone else within the department who has authority to manage that account. The justification of redirecting the messages should be clearly established prior to redirection. The duty of confidentiality should be impressed upon the member of staff who receives the redirected mail.

General Rules

Properly used, email can be an immense benefit to the NHS and its staff. The following rules apply to anyone using the Trust's IT systems to send and receive email and the posting of information on the Trust's Web Pages:-

- Confidential person-identifiable information should not be distributed by email unless there is a specific requirement for it. Casual disclosure of personal details of patient, employee, volunteer or contractor without just cause may be considered a breach of personal privacy as defined under the Data Protection Act.
- If however you need to send such information see the **'Secure Email Guidance'** document (on SID) for clear direction on what secure method to use.
- Log in at least twice daily, if not all day, and respond to requests within a reasonable time.
- Advise people when you are not available. Use the tools within your system (i.e. Out Of Office Assistant) to notify others of your inability to read your email.
- Set up a Signature with your name, organisation, telephone number, other useful contact information and a legal disclaimer.
- As people may receive many email messages it is important that a subject is added to the email in order that the recipient can clearly see what the email is about. It will also assist the recipient in prioritizing opening of emails.
- Ensure that you are sending the email to the correct person. If in doubt, confirm their email address with them.
- Use the spell checker before you send out an email.
- Emails should be treated like any other correspondence and should be replied to within an acceptable time limit.
- Only send emails if the content would be suitable for display on a public notice board or the Trust's publication scheme. If they cannot be displayed publicly in their current state, consider rephrasing the email or using other means of communication.
- Use distribution lists with care – is it important that all addressees receive the email? Only use organisation-wide distribution lists to communicate important business information that has genuine site-wide value.
- Update your email groups at regular intervals. Check for leavers or members who have moved on into another role – it may not be appropriate for them to continue to receive emails from the group and may lead to a breach of the DPA.

- Type your message in lower case. Using capital letters is considered aggressive.

Do's and Don'ts of Email

- Staff must not send any message which is abusive, offensive, obscene or potentially defamatory or which consists of gossip. Comments of this nature can be construed as harassment. Ensure that all statements and comments you make about people or organisations are true (*Computer Misuse Act 1990*).
- Remember that the email system is for business use. You may, however, make sensible use of it for non-business purposes. Use your common sense if you send personal messages to other members of staff via this system. Bear in mind that you should not be spending more than a minimal amount of time on matters unrelated to your work. Be aware that unauthorised and excessive use of any means of electronic communications by staff at the Trust is a disciplinary offence.
- Take extreme caution when disclosing your Trust Internet email addresses to outside organisations. The addresses may be misused or sold on and as a result cause an influx of junk mail.
- Do not circulate jokes; computer programmes (executable files) documents such as chain letters, celebratory greetings messages (e.g. animated Christmas cards), music, video and photographs. Circulating such material can pose serious business and operational risks by using up excessive storage space and may infect PCs or servers with viruses.
- Anonymous messages are not permitted. Do not attempt to send messages purporting to come from another individual or email account without written consent.
- If you send personal messages you must take care that they cannot be confused with Trust business communications.
- Do not present views on behalf of the Trust, unless you are authorised to do so
- Be mindful when deleting emails permanently, as under the Freedom of Information Act, you may need to refer back to such communications or provide as evidence in responding to Freedom of Information requests.
- Do not send large attachments by email. Place large attachments in a shared location (where possible) and then send just the file path via an email. If you believe that most recipients will print the document, try to use another method of sending the hard copy.
- Do not attach files to emails from unknown sources (may contain viruses). Do not open file attachments with possible virus warnings. If you suspect you received a virus by email, telephone the SSHIS Service desk immediately. Do not attempt to remove the virus yourself. The Service Desk will need to know what virus it is.
- Keep the Inbox to a minimum and adhere to good housekeeping practices. Create a personal folder structure under different headings. Transfer email from the Inbox to the appropriate folder on regular basis.
- Review saved emails every month and delete any that are no longer required. If there is an email that may be required in the future, it should be archived.

IT Access to Email Messages

SSHIS do not routinely monitor individual email accounts or email messages. However, in order to maintain the availability of the email system, there may be occasions when the SSHIS have to access a mailbox for maintenance and housekeeping purposes e.g. if a mailbox has reached its maximum size, staff changes etc. Such access will not be used to review the content of individual email messages.

Individuals' Rights to Access Email Messages

The Data Protection Act gives individuals the right to access any information held on them, including email messages. (*Access to Health & Employee Records Policy 7.02*). In

addition, the Courts and Employment Tribunals have the power to order disclosure of emails that may be relevant to a case. This emphasises the point that emails are more than just an electronic conversation. Messages should be taken seriously and the content should be in accordance with the principles of the Data Protection Act, GDPR and the Caldicott recommendations.

Malicious Communications

See also ISD J – Secure Email Guide - page 23

The Malicious Communications Act 1988 makes it illegal in England and Wales to "send or deliver letters or other articles for the purpose of causing distress or anxiety".

a) a letter, electronic communication or article of any description which conveys—

   i. a message which is indecent or grossly offensive; a threat; or

   ii. information which is false and known or believed to be false by the sender; or

b) any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature,

Is guilty of an offence if his purpose or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

Copyright

Email messages may contain or attach copyright work owned by a third party. If you make an electronic copy of such work you may be infringing copyright (Copyright, Patents & Designs Act 1988). It is an offence to copy any item of software without the owner's prior permission. The use of illegal or unauthorised software on a Trust computer is a breach of this policy.

INFORMATION SECURITY DOCUMENT F

INTERNET ACCESS

All sections of this policy apply to all Internet access using any NHS resources. Violation of this policy will be grounds for having access to the NHSnet and Internet restricted or revoked.

It is clear that Internet access can be a valuable tool to staff throughout the Trust, both within their normal work activity and as an aid to learning. Furthermore, the Internet is also a route by which to deliver information and guidance to patients and to the public.

Potential Problems

There are a vast number of sites that the Trust would not wish employees to access. We must equip ourselves with a set of security measures which will minimise the risks to our resources from external intruders and which will both deter and detect employees who access 'inappropriate' Web sites. The definition of 'inappropriate' is anything that may cause offence to other individuals. **The Trust has the ability to monitor Web sites that user's access and does so on a regular basis.** It is the responsibility of a user's line manager to give the user Internet access rights or to take those rights away.

Breaches of this policy will be brought to the attention of a user's line manager and to the appropriate senior manager.

Responsibilities of the User

It is the responsibility of all staff within the Trust to ensure that the computer systems and the data that is accessed through them are safe and secure. Staff that uses the Internet have additional responsibilities relating to security, confidentiality and inappropriate use.

Permissible Access

Access to the Internet is primarily for healthcare related purposes. That is for Trust work or for professional development and training. Reasonable personal use is permitted provided that this does not interfere with the performance of your duties and is carried out during official work breaks e.g. lunchtime or outside of core working hours. The Trust has the final decision on deciding what constitutes excessive use.

Non-Permissible Access

No member of staff is permitted to access; display or download from Internet sites that hold offensive material; to do so may constitute a serious breach of Trust security and could result in dismissal and/or criminal prosecution. Offensive material is defined by the Trust's Equality of Opportunity in Employment policy and Harassment at Work policy and includes hostile text or images or inappropriate website access relating to gender, ethnicity, race, sex, sexual orientation, religious, cultural or political convictions and disability. Users must not create, store or distribute any material that is libellous, blasphemous or defamatory. This list is not exhaustive. Other than instances which demand criminal prosecution, the Trust is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet.

Unintentional Breaches of Security

If you unintentionally find yourself connected to a site that contains sexually explicit or otherwise offensive material, you must disconnect from the site immediately and inform your line manager and the IT Service Desk.

Accessing the Internet via Mobile Devices

When staff access the Internet or World Wide Web using mobile computing devices such as SmartPhones or Tablet PCs and that access is gained using a Trust network (including wireless), an audit trail of sites visited is maintained centrally by the IT Service. When access is gained through a home broadband connection, an audit trail may remain on the device.

INFORMATION SECURITY DOCUMENT G

INFORMATION SECURITY RISK MANAGEMENT & INCIDENT REPORTING PROCEDURE

(Policy 4.18a Risk Management Policy).

The objective of information security risk management is to ensure that information security breaches are detected, reported and investigated. The objective applies to both manual and computerised information.

Risk management is recognised within the Trust as an integral part of good management practice and the Trust has a systematic approach to identifying what goes wrong in patient and non-patient areas and why and learning lessons from these events to ensure that action is taken to prevent a re-occurrence.

An information security incident is defined as an event, which has resulted, or could result in:

- The disclosure of confidential information to any unauthorised individual. This includes manual and computerised information.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.
- An adverse impact, for example:
  - o embarrassment to a patient
  - o embarrassment to the NHS
  - o legal obligation or penalty
  - o disruption of activities
  - o financial loss to the Trust
  - o threat to personal safety or privacy

Some examples of security incidents are:

- An IT system becoming infected with a computer virus.
- A user's password becoming known to other persons and used to access systems without authorisation.
- Unauthorised access to confidential information/data, i.e. smartcard left in machine to be used by another member of staff.
- Theft of computer hardware or health records containing patient-identifiable information

All Information Security incidents and near misses should be reported on the Trust Safeguard Incident Reporting System.

Non-Incidents – Confidential Documents received in error

- There are occasions where confidential information is sent to the Trust in error by other organisations. Whilst these are not strictly speaking an incident to be added to Safeguard, as they are not our breach, we have taken the decision to monitor them. Should we then be questioned by any authority at a later date we can show due care by behaving responsibly and notifying the senders and the Information Security Department involved.
- Any such information you receive should therefore be logged on the Register held by the Information Security Manager and IG Manager.
- **Do not forward the mail you have received as this may result in a further breach (by our Trust).**
- A simple email giving the date, person/organisation and your response will be sufficient for the register.

INFORMATION SECURITY DOCUMENT H

VIRUS CONTROL PROCEDURES

A virus is a self-replicating piece of software that will spread throughout a computer or a network of computers when an infected file is exchanged. The effects can be very damaging to systems and can also impact heavily on the Trust staff. Virus removal is costly and takes time. Whilst the machine is being disinfected colleagues are prevented from accessing their key clinical and business critical application.

The Trust, therefore, must take appropriate action to:-

- Minimise the threat of a virus infection.
- Manage the problems by maintaining the currency of the protection through regular upgrades.
- Provide remedial actions.

An anti-virus solution is installed onto all networked, stand-alone or portable computers. Anti-virus installation is a mandatory requirement. Removal of such software is not permitted. Individuals are responsible for ensuring that anti-virus software is installed and active. Advice is available from the SSHIS Service Desk.

If you send an attachment that contains a virus, you and the Trust can be held liable. SSHIS maintains up-to-date virus protection software on the network which is designed to protect your system. There area however a few simple rules which can help us all.

- Do not forward e-mails from unknown sources.
- Do not open email attachments from unknown sources
- Do not attach files to emails from unknown sources (may contain viruses).
- Do not open file attachments with possible virus warnings.
- If you suspect you received a virus by email, telephone the SSHIS Service Desk immediately.
- Do not attempt to remove the virus yourself. The Service Desk will need to know what virus it is.

Spam, Chain Mail, Jokes and Unsolicited Messages

Spam is the name given to large quantities of junk emails that are sent to an excessive number of recipients. Software to filter out suspected spam emails has been installed on your computer. Whilst this software is reasonably effective, new ways of disguising spam messages are being invented all the time, meaning that some messages will still get through the protection. You should also be aware that some genuine messages will be identified by the system as possible spam and placed in the Junk E-Mail folder of your mailbox. You should check the contents of this folder regularly and delete any messages that are not required.

Individuals who repeatedly forward messages of this type using the Email system will be reported to the HR Department for the consideration of disciplinary action. The IT Service will delete any messages of this type whenever they are discovered.

Cyber Crime, Phishing etc.

The NHS is increasingly targeted by outside organisations and individuals maliciously seeking information or access to our systems. Staff need to be mindful of the threats and report any suspected instances to SSHIS.

INFORMATION SECURITY DOCUMENT I

"SMARTCARDS" *(Policy 7.22 Registration Authority)*

NCRS Acceptable Use, Terms & Conditions

The NHS Care Records Service Registration Authority is responsible for registering and verifying the identity of NHS staff that need to use the NHS Care Records Service and related IT systems and services, including Electronic Staff Record (ESR), eReferrals and the Electronic Prescriptions Service.

Access to these computer systems and services is controlled by smartcards with photographic ID and passcode, similar to a chip and pin credit card. Your card lasts for the duration of your NHS employment, no matter where. Registration Authorities issue smartcards to authorised staff with an approved level of access to patient information. See link below http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf

To obtain a 'smartcard':

- complete an application form (RA01partb) http://nww.hscic.gov.uk/rasmartcards/docs/ra01b.doc
- with the support of your manager or an approved sponsor agree what level of access to the system is required for your particular role within that organisation,
- have a face-to-face meeting with the Registration Authority Team to process the registration, take a digital photo and issue the Smartcard.
- Individuals will have to provide the minimum of 3 items of identification as per national guidance http://systems.hscic.gov.uk/rasmartcards/documents/nhsemplidcheck.pdf

Important to note that failure to provide the appropriate identification at this meeting, the Registration Authority Team will be unable to process the registration request. When the card has been issued, the smartcard will contain information about the individual and their access rights to National Spine Applications. Please note that no clinical access is ever assigned to an individual's smartcard profile unless they have attended and completed the appropriate Clinical System Training. The smartcard must be treated with great care as it allows access to confidential patient informational and for organisations that are ESR enabled this give access to individuals personal information such as Pay, Annual leave, sickness etc.

The Smartcard is the responsibility of each staff member and it must be brought to work whenever you are on duty. It is not an identity card.

Remember – treat your smartcard with the same care as your bank card

- Do not leave logged-in workstations unattended.
- Do not leave smartcards unattended.
- Do not share smartcards or passcodes with other users.
- Do not apply for or use more than one card.
- Use only IT equipment that has been provided by the NHS and not, for example a shared home PC.
- Ensure that printouts or other outputs are appropriately protected and disposed of when no longer needed. Printouts may not be copied, removed from the workplace or shared with others without the proper authorisation.
- Contact your local RA Agent to re-set a forgotten pin number

INFORMATION SECURITY DOCUMENT J

Transmission of Person Identifiable Data (PID)

The Data Protection Act places additional responsibilities on all staff to obtain and process health data fairly, with the knowledge and agreement of patients.

Additional care must be taken when transferring person identifiable data (PID) between NHS and partner organisations.

- The transmission of PID should be kept to an absolute minimum and must be provided on a strict need-to-know basis.
- This policy does not cover the transfer of patient records (*Policy No 7.7 – Records Management Policy*).

Fax Transmission of PID

See Goldfax Guidance document on SID

The Trust does not support the use of fax machines. Instead employees may use the Goldfax solution on Outlook, following the Safe Haven principles of checking the efax address and contacting the destination, prior to sending, to ensure the information is going to the correct person. *(see also Policy 7.14 Safe Haven Policy)*

Email Transmission of PID

See **Secure Email Guidance document on SID** for the full guidance as briefly described below:

Firstly – if sending personal information, remember to check you are sending the email to the correct person. Then work through the three step process below following the Secure Email Guidance document on SID

1. Secure Domain
   Check the list in Appendix A of the Guidance document.
   If the organisation you wish to send to is included you do not need to encrypt your document as we have internal secure connections between our email servers and theirs.

OR

2. NHS Organisation
   You will need an NHS.net account in your name and the address of the NHS.net account you are sending to. Please ensure you use these accounts only. **Do not send to NHS.net from your North Staffs account as this removes the encryption**. *(There are a few non NHS organisations using the NHS.net service – listed under a separate heading in Appendix A of the Email Guidance Document on SID)*

OR

3. Non NHS Organisation
   For all other email you will need to activate the 'Sophos' software on your Outlook email account to encrypt your message. This is simply done by following the steps detailed in the Secure Email Guidance Document.

*Should any loss or suspected loss of PID occur, this must be reported in accordance with the Trust's Incident Reporting Policy (see also **ISD G - Information Security Risk Management & Incident Reporting Procedure**).*

INFORMATION SECURITY DOCUMENT K

Software Licensing Procedure

Unauthorised Installation of Software

Unauthorised software poses a risk to your computer, other computers and the network as a whole from malicious code embedded within the software. The risk applies to all programs and games downloaded from the Internet, on disk, CD/DVD or any other storage media. Malicious code may be computer viruses and spyware, and the effects will vary depending on which has been downloaded.

A second and equally important reason why you should never use unauthorised software is because of licensing issues. The Trust is required to purchase licenses for the use of all software on its systems. If you install software without authorisation this process is by-passed and you put the organisation at risk of legal action from the owner of the software. If you are installing so-called free software it could be an illegal copy, or it could be trial software with an expiry date. Even if neither of these things apply, the software is likely to be for single personal use and require a license for corporate use.

Individual Responsibilities

Individuals must not install software on to a Trust owned desktop or laptop computer and doing so constitutes a disciplinary offence. SSHIS audits all computer equipment including software. If unauthorised software is found on a system or if no license agreement has been purchased, IT staff are authorised to remove the software.

Should you suspect the presence of unauthorised software on your system you should report it to the SSHIS via the Service Desk.

SSHIS/IT Staff Responsibilities

SSHIS will maintain a Definitive Software Library (DSL) that contains the authorised version of all software in use. Only authorised software will be accepted into the DSL. The library is located in the IT Department and access to it is strictly controlled.

SSHIS will carry out a reconciliation of software licenses at not less than 12 monthly intervals to verify that the number of licenses held matches the number of equivalent software installations. The results of the software audit will be made available to Trust managers and all anomalies investigated and corrected.

INFORMATION SECURITY DOCUMENT L

Encryption of Mobile Devices *(Policy7.19 Mobile Working)*

In accordance with NHS Security Procedures and best practice guidance, all mobile devices that are capable of storing data will be encrypted.

This is to ensure that in the unfortunate event of a device being lost or stolen, any data stored on it cannot be read without first entering a password.

Devices covered by this policy

- Laptop Computers
- Notebook Computers/Tablets
- USB Memory Sticks
- Digital Cameras
- Mobile Phones/Smartphones/iPhones
- Personal Digital Assistants (PDAs)
- CD/DVD Writers
- Micro SD Cards
- Scanners

N.B new storage devices are being invented all of the time. The above list is not exhaustive. Any device which can store data is covered by this policy.

Saving to Data Storage Devices

Access to a CD/DVD write facility is restricted on all devices. All staff may read data from electronic storage devices but only named individuals are able to write data to these.

SSHIS/IT Staff Responsibilities

All new mobile computing devices (laptops, notebooks) received by IT Services are to be encrypted during the build process and before delivery to the customer. Individual procedures applicable to each device type are available from the SSHIS Desktop Support Manager.

All other devices will be encrypted by the user on first use (see below).

User Responsibilities.

Any official NHS mobile device that you connect to the network must be encrypted. Software has been installed that will scan such devices as soon as they are detected. If the device is not encrypted, the software will prompt you to do this. Failure to follow the on-screen instructions will result in the device becoming unusable on the network.

Non-NHS devices (for instance personal digital cameras, MP3 players etc.) should never be connected to the network. This includes direct connection through a PC/Laptop via the USB port or inserting an SD (Storage Disk) card into peripheral devices such as printers. If you do decide to connect a personal device, you will be prompted to encrypt it. Once this has been done, you will not be able to reverse the process. The IT Service accepts no responsibility for damage caused to personal equipment through failure to adhere to this policy.

Some devices such as USB Memory Sticks can be purchased pre-encrypted. These devices are approved for use on the network.

INFORMATION SECURITY DOCUMENT M

Social Media & Social Networks *(Policy 7.19 Mobile Working)*

The term Web 2.0 is commonly associated with web applications that facilitate interactive information sharing and collaboration on the World Wide Web. A Web 2.0 site gives its users the free choice to interact or collaborate with each other in a social media dialogue as creators in a virtual community, in contrast to websites where users are limited to the passive viewing of content that was created for them. Examples of Web 2.0 include social-networking sites (e.g. Twitter, Facebook, MySpace, YouTube etc.), blogs, wikis, video-sharing sites, hosted services and web applications. Internal SharePoint sites (e.g. Staff Information Desk) also provide social networking capabilities and are included in this policy.

North Staffordshire Combined Healthcare NHS Trust has the right to manage its reputation on all levels, including any employee interaction on social networking sites that could possibly reflect an opinion upon the Trust. All employees of NSCHT agree to the following guidelines:

- You must differentiate your private online persona from any work persona. This means that you should only register on a Web 2.0 site using your private (non-NHS) contact details unless you are specifically representing the Trust.
- Act appropriately and respectfully on all social networks. Your online presence is a reflection on the organisation, whether or not you have stated your employment with the NHS or your specific Trust.
- Any information published online, in any capacity, is subject to disciplinary action or in severe cases, termination.
- All information published on the Web should be in accordance with the Trust's confidentiality agreement.
- Do not discuss or disclose confidential information without your manager's expressed consent. Never use social networks as a means of relaying confidential information.
- Respect copyright and plagiarism laws on social networks. In instances of any violation of these laws on your social networking sites, the Trust is not liable.
- Blogs and other online journals should express a clear disclaimer that the views expressed in the blog are the author's alone and do not in any way reflect the views of North Staffordshire Combined Healthcare NHS Trust.
- Access to the Internet is primarily for healthcare related purposes; that is for Trust work or for professional development and training. ***Reasonable*** personal use is permitted provided that this does not interfere with the performance of your duties and is carried out during official work breaks e.g. lunchtime or outside of core working hours.

Note: These guidelines apply to all methods of accessing Web 2.0 sites. This includes Trust-owned or Personal Computers, Smartphones, Tablets, iPads etc.