

# Information Governance and IMT Security Policy

Version number :	5.8
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	IGSG Chair's Action
Ratified by:	IGSG Chair's Action
Date ratified:	21 April 2021
Name of originator/author:	Head of Information Governance
Executive Director lead :	Chief Quality Officer
Implementation Date :	April 2021
Last Review Date	April 2021
Next Review date:	April 2024

Services	Applicable
Trustwide	X
Mental Health and LD	
Community Health Services	

## Version Control Summary

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Status</b>	<b>Comment</b>
1.0	April 2002		Final	Approval by DPA/Caldicott Steering Group as an IM&T Security Policy
2.0	May 2002		Final	Issued in draft to JSC for consultation and comment
3.0	May 2002		Final	Approved
4.0	May 2005		Final	Modifications for internal review to reflect new Healthcare Governance Arrangements, responsibilities, clarity on procedure for requesting access to information stored on IM&T resources
4.1	November 2005		Draft	Additions/modifications as a result of national IG toolkit requirements, committee name changes. Inclusion of an Information Governance Policy Statement, additional detail on Network Security, Equipment disposal and Safe Haven Fax Management
4.2	November 2005		Draft	Minor changes and new title following review, discussion and approval at Information Governance Steering Group in Nov 2005
4.3	March 2006		Final	Minor revisions re Indemnity condition to Contractors Letter

5.1	December 2007		Draft	Update following internal review and additional national guidance - Dec 2007
5.2/3	Jan / Feb 2008		Draft	Added bullet point to "8. Computer and Network Operations" - "Code of connection" (page 23) for unsecured network devices and reference to CfH Statement of Compliance (SoC) standards  Added Appendix F "The connection of unsecured devices to the trust network"
5.4	March 2011		Draft	Roles & responsibilities updated
5.5	April 2014		Draft	Updating and Housekeeping of Policy
5.6	November 2015		Draft	Annual review + change the word "Should" to "Must" to stop implying optionality
5.7	March 2019		Draft	Inclusion of pseudonymisation in section 16 of the document. Updated to reflect changes in data protection law
5.8	February 2021		Draft	Updates regarding use of tracked / recorded delivery for the transfer of original documents containing personal identifiable information via post

## Contents

<b>Paragraph</b>		<b>Page</b>
1	Executive Summary	7
2	Purpose	7
3	Duties	7
4	Job roles	9
5	Principles	10
6	Confidentiality agreement	12
7	Confidentiality and research	13
8	IM&T security policy	13
9	Legislation	14
10	Asset management	14
11	Access control to secure areas	16
12	Equipment security	16
13	Computer and network operations	18
14	Security incident management	19
15	System planning and procurement	21
16	Protection from Malicious software	21
17	Housekeeping	22
18	Data and software storage and exchange	22
19	General principles relating to person identifiable information	24
20	Consent	25
21	Local policy	27
22	Sharing of Personally Identifiable Information	27
23	Transfer of information	28
24	Pseudonymised information transfer	29

25	Legislation and Guidance on Using Person Identifiable Data	30
26	User access control	32
27	Computer access control	34
28	Application access control	35
29	Disposal of IM&T Equipment	36
30	Data validation	37
31	Business continuity Planning	37
32	Compliance	38
33	Risk assessment	39
34	Safe haven principles	40
35	Network security policy	41
Appendices		
Appendix A	Asset Register	49
Appendix B	Information Assets – Requirements for Classification	50
Appendix C	Summary of Objectives	51
Appendix D	Pro-forma required from Third Parties	54
Appendix E	The Connection of Unsecured Devices to the Trust Network	55
Appendix F	General Management of Laptops	56

## **1.0 EXECUTIVE SUMMARY**

This document sets out a combined Information Governance and Security Policy and standards for information asset management and data security across the Trust.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of staff, services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore important to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

## **2.0 PURPOSE**

To set out the standards for information governance, data security and information management and technology to ensure robust and appropriate management of the Trust's information assets.

## **3.0 DUTIES**

### **Trust Board & Chief Executive**

The Trust Board and Chief Executive are legally responsible for information governance and information security within the Trust. It defines the Trust's policy in respect of information governance and information security, taking into account legal and NHS requirements. The Trust is the data controller for the information it processes including data registration responsibilities, duties to monitor and ensure adherence with lawful practice and powers to appoint data protection supervisors.

### **Quality Committee**

The Information Governance Steering Group (IGSG) will report to Quality Committee twice yearly. Quality Committee ratifies information governance policies after their approval at IGSG. Additional reports may be tabled on an exception basis.

### **Information Governance Steering Group**

The Information Governance Steering Group is responsible for overseeing day-to-day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Trust and raising awareness of Information Governance. Membership is comprised of the Chief Quality Officer (Chair) SIRO, Caldicott Guardian, subject specialists and locality representatives. Locality representatives are required to ensure views and decisions are communicated to their teams and acted upon.

## **Executive responsibility for information governance**

The Chief Quality Officer holds the portfolio for information governance and chairs the Information Governance Steering Group.

### **Senior Information Risk Officer (SIRO)**

The SIRO is the Chief Financial Officer and ensures information risks are reported, assessed, mitigated and appropriate actions taken. The SIRO chairs the Digital Board and holds the portfolio for IMT.

### **Caldicott Guardian**

The Chief Medical Officer is the Caldicott Guardian and responsible for ethical advice and decision making regarding information processing and sharing, who is the Trust's Senior Information Risk Officer (SIRO) and as such works closely with the Caldicott Guardian, Associate Director of Assurance, Associate Director of ICT, Associate Director of Information Governance, and the Information Governance Steering Group generally to ensure risks are appropriately reported, assessed, mitigated and appropriate actions taken.

The Caldicott Guardian is supported by the Deputy Medical Directors who fulfill the role of Deputy Caldicott Guardians

### **Data Protection Officer**

The Associate Director of Information Governance fulfills the legal role of Data Protection Officer. The post holder is responsible for the control, development and strategic direction of information governance. The overall responsibility for maintaining and implementing the Trust's Information Governance and IM&T Security Policy lies with the Associate Director of Information Governance.

The post holder is responsible for identifying information systems and physical and logical sets of data and for assigning an owner to the information system and the physical and logical sets of data.

### **Chief Digital Officer**

The Chief Digital Officer (CDO) is responsible for the security of IM&T resources and systems and for technical data security.

### **Managers**

Managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

### **Information Asset Owners (IAOs)**

Service Directors are Information Asset Owners for the information assets held in their localities and as such are responsible for ensuring the security, processing and data flows of their assets. IAOs are responsible for assessing and mitigating any risk associated with their assets.

The responsibility for managing security of physical patient records resides with the relevant Service Directors in each locality, service area or function (e.g. Human Resources) of the Trust managing and holding those records.

### **Information Asset Administrators (IAAs)**

Team managers are normally responsible for the day to day management of their information assets and must ensure their use is appropriate.

### **Electronic Systems Managers**

Individual information systems, irrespective of form (e.g. electronic or physical), that hold sensitive information, will have identified individual System Managers (SMs). These individual System Managers will ensure information security is maintained to the standards set out in this policy. System managers are responsible for ensuring the integrity of their information systems.

### **All staff**

All staff using information systems within the Trust must follow the instructions and guidance in this policy. All staff with access to information systems that hold or process person identifiable information has a common law duty to maintain the confidentiality of that information. As such all members of staff have a duty to follow all instructions from the IGSG and nominated System Managers, IAOs and IAAs.

## **4.0 JOB ROLES**

The Trust has an obligation to reduce the risks of human error, theft, fraud or misuse of facilities and to ensure that users are aware of information security threats and concerns, and are equipped to support the Trust's security policy in the course of their normal work.

Security must be addressed at the recruitment stage and be included in job descriptions and contracts, and monitored during employment.

Job definitions must define security roles and responsibilities as laid down in the Trust's Information and IM&T Security Policy.

Managers must ensure that where a staff member is required to use Information IM&T services, systems and paper records that, according to their responsibilities they are briefed on the Trust's Information and IM&T Security Policy, associated legislation including the Data Protection Act 2018, GDPR, Computer Misuse Act (1990) etc. Staff must also be briefed on Caldicott guidance and be made aware of conduct and disciplinary procedures which may be invoked if a breach of security arises.

Each member of staff is personally accountable for the function he/she performs. Where practical, there must be segregation of functions and separation of duties so that tasks which have a security element are not performed by the same person so that threats to security are averted.

Control of a job function that could allow fraud or theft must be part of the job responsibility of at least two people. Staff can then be rotated on an irregular (unpredictable) basis.



It is essential that significant work performed by a key individual can be taken over by someone else in the event of the unavailability of the key person. Dependence on key people may be reduced by the use of documentation.

Expertise must be shared and for critical systems, training must be given to at least two people so that in the absence of one, the other may pick up work in the critical area.

Each individual must know the extent of his/her authority, ranging from individual tasks to budgetary responsibility.

Information and IM&T security privileges and access rights must be allocated on the basis of the specific job function. Privileges and access rights must not be based on the status of the job.

Personal interest must be declared in circumstances where it could lead to a conflict of interest. This could be the case where IM&T procurement is involved.

Contract staff must be informed of the Information and IM&T security procedures and must sign an agreement, be trained in data security, have the same codes of conduct and discipline as permanent staff. Where Staff are taken on through an agency the conditions must form a part of the contract of engagement with the agency. If work is of a more sensitive nature and carried out by contract staff - e.g. computer maintenance - then extra conditions must be identified and imposed in accordance with this greater risk exposure.

Reference requests during recruitment must also indicate Information and IM&T security matters.

## **5.0 PRINCIPLES**

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance

- Information security
- Quality assurance

### **Openness**

- Non-confidential information on the Trust and its services must be available to the public through a variety of media, in line with the Trust's code of openness
- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness
- Patients must have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Trust will have clear procedures and arrangements for handling queries from patients and the public

### **Legal Compliance**

- The Trust regards all identifiable personal information relating to patients as confidential
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act, GDPR and the common law duty of confidentiality
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

### **Information Security**

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training

- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security
- All guidance and standards on the security of data cover records held and managed for patient, staff and carers receiving service from or employment by the Trust

### **Information Quality Assurance**

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality must be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

## **6.0 CONFIDENTIALITY AGREEMENT**

All users of data, records, IM&T equipment and systems must sign a non-disclosure undertaking (confidentiality agreement). This undertaking must form part of the contract of employment with the member of staff. The conditions in the undertaking must be clearly explained. Third party contractors working for the Trust must be required to sign the proforma agreement included at Appendix D

Where agency and contract staff and other third party users are not already covered by a non-disclosure undertaking in their existing contract they must be required to sign such a confidentiality agreement before they are connected to the Trust's IM&T facilities.

Confidentiality agreements must be the subject of review where there are changes to terms and conditions for employed staff or other contractors' employment.

When an employee leaves:

- the ICT department must be informed
- The manager must confirm that the confidentiality agreement will continue to apply even though the person is leaving.
- Passwords to affected systems must be changed to deny access.

- Relevant departments must be informed of the changes.
- The name must be removed from Trust lists.
- Reception staff and security guards must be informed of the termination to ensure that the person must now be treated as a visitor.
- where possible staff working out a notice period must be assigned to non-sensitive tasks or otherwise appropriately monitored.
- Trust property must be returned, particularly personal identification devices, entry keys and other access items.

Particular attention must be paid to the above if the termination is not 'amicable'. The relationship between the employee and the person leaving must be assessed so that the extent of the implementation of the 'leaving measures' can be carried out at an appropriate level. E.g. a staff member leaving on good relations may retain all privileges until the day of leaving.

## **7.0 CONFIDENTIALITY AND RESEARCH**

Preserving the confidentiality of service users or volunteers enrolled in a research programme demands the same precautions and attentions as those outlined throughout this document with regard to service users and staff. The following additional requirements must, however, be assured:

a) Where access to medical records is required, the researcher must provide:

- The reason for requesting access and steps to be taken in order to maintain confidentiality
- Names and status of those needing access to notes: each must sign a declaration of confidentiality
- The specified period of time during which access will be required
- Confirmation that service users/volunteers will be coded and not identified

b) Where direct contact with service users/volunteers is involved, signed consent must be obtained from each individual enrolled in compliance with the Research Governance Framework. Consent forms may be subject to audit.

Under the Data Protection Act, research data held on a computer or as a paper record must be registered for data protection purposes. However, as an employee or honorary contract holder of the Trust, a researcher is automatically included in the organisation's registration.

## **8.0 IM&T SECURITY POLICY**

The NHS IM&T Security Manual describes the need for an IM&T security policy as follows:

"Data stored in information systems represent an extremely valuable asset. The increasing reliance of the NHS on information technology for the delivery of health care makes it

necessary to ensure that these systems are developed, operated, used and maintained in a safe fashion.”

### **The purpose of the security policy**

The policy has been developed to protect the organisation from hazards and threats to ensure that the information held in Trust systems is secure from accidental or deliberate unauthorised modification or disclosure. The terms “systems” and “data” used in the context of this document refer to information in held in either electronic or paper formats. The terms ‘information assets also includes stored paper records.

The security policy is intended to preserve confidentiality, integrity and availability of data.

- Confidentiality involves the limitation of data access to those with specified Trust authority to view the data
- Integrity is the requirement to ensure that all system assets are operating correctly according to specification and in the way the current users believe they must be operating.
- Availability is the requirement to ensure that information is delivered to the right person when it is needed.

## **9.0 LEGISLATION**

UK legislation and EU directives also govern information and IM&T security. The most significant legislation in this area is:

- The Data Protection Act (2018), which has superseded the 1998 Act
- The General Data Protection Regulation (GDPR)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

## **10.0 ASSET MANAGEMENT**

All major assets must be accounted for and have a nominated owner for security purposes. Owners must be responsible for maintaining appropriate security measures. Responsibility for implementing security measures may be delegated, but accountability must remain with the nominated owner of the asset.

Information security classifications may be used to indicate the level and priority of security protection. These classifications are: -

- Extremely sensitive (class 1): where data held is of a highly sensitive nature and where security is at the highest level, e.g. data relating to specific patients in highly sensitive specialities (sexual health, mental health).

- Sensitive (class 2): where data is not of the most sensitive nature but still requires strict security, e.g. all patient data in specialities other than those in class 1.
- Ordinary (class 3): where data is not patient based but nevertheless security is required. Data in this class will normally be aggregated or lists, e.g. Mailing lists, staff or GP lists.

### **General principles of asset ownership**

Each logical or physical set of data must, for security purposes, be assigned an owner. The owner will be responsible for:-

- identifying all the data within the area of responsibility
- specifying how the data can be used
- agreeing how the data can be used
- agreeing who can use the data
- agreeing what type of access each user is allowed
- determining the classification (class 1, 2 or 3) of the data
- reviewing the classification
- approving appropriate security protection
- ensuring compliance with security controls
- ensuring compliance with legislation covering personal or medical data
- Ensuring compliance with Data Protection Act - through the contact for Data Protection.

Classified information will be labelled (either Class 1, 2 or 3) and output from systems (including printed reports, magnetic media, electronic messages and file transfers) must also be labelled with the classification.

Where data is mixed in classification, the most sensitive will be used.

The review process will check for appropriateness of classification. As over- classification may lead to unnecessary expense, review must be carried out periodically. For example where data has been made public it ceases to be sensitive.

Unless specifically identified in this inventory of assets, equipment sited within a department or directorate will be the responsibility of the director or head of that department. This will generally mean that the responsibility for security of PCs (including processor and monitor), printers and similar 'client' based kit will rest within the directorate where the kit is held and used.

Directorates or departments which have the majority of use of an application and similar software will be identified as the owner of that application or software. The data, which results from the use of that application, will also be owned by the same directorate or department.

## **Ensuring confidentiality of extremely sensitive information**

All information that requires a Class 1 (extremely sensitive) classification must be identified and each Directorate needs to take appropriate steps to ensure its security and confidentiality. Departmental Directors will be the Confidentiality Custodian for Class 1 information held within their Directorates. All other information must be deemed to be Class 2/3 confidential.

### **11.0 ACCESS CONTROL TO SECURE AREAS**

IM&T facilities supporting critical or sensitive business activities must be housed in secure areas. These facilities must be physically protected from unauthorised access.

#### **Physical security perimeter**

Physical security protection for the Trust is based on defined perimeters and achieved through barriers within the organisation. Critical installations must be protected at least by lock and key.

IT equipment is held in various office locations across the Trust's estate and externally where clinical services are undertaken on non-Trust premises. Each office area that contains an IM&T database or equipment will be controlled in office hours by an approved locking or entry system and out of hours by an agreed access mechanism.

A security guard service will be provided out of office hours to ensure 24-hour protection of accommodation.

#### **Challenging strangers**

Staff are given instruction to challenge people who are visitors or otherwise unknown to them.

### **12.0 EQUIPMENT SECURITY**

Equipment must be physically protected from security threats and environmental hazards.

Protection of IM&T equipment is necessary to reduce the risk of unauthorised access to data and to safeguard against loss or damage. Attention will be given to the siting and disposal of equipment.

Special measures will be taken as appropriate to protect supporting facilities, such as electricity supply and cabling infrastructure.

#### **Equipment siting and protection**

A computer environment, including temperature, humidity and power supply quality is available and used for corporate systems.

Corrective action will be taken when detected - normally on behalf of the Trust by ICT staff - using maintenance support arrangements.

The Trust operates a no smoking policy

Eating and drinking are not allowed in designated computer rooms, or in any office areas in close proximity to an IM&T database, and are to be avoided by staff using computer equipment.

### **Security of equipment off premises**

Equipment taken off site must only be done with the approval of the appropriate manager. Portable electronic devices must be encrypted. Staff who have obtained authorisation to take equipment off site must ensure that such equipment is given a high level of protection. **Equipment must not be left in cars etc as the high incidence of car theft leads to a substantial level of risk for the Trust's equipment and data.**

All laptops must be connected to the Trust network on a monthly basis to ensure the appropriate updates, system security and passwords are updated.

Systems engineers allowed into the premises must identify themselves as belonging to the maintenance company. The engineer will adhere to the general procedures adopted for all visitors and where possible will be handed over to the department for whom the work is to be undertaken.

Where a data medium (e.g. disk, tape) is removed from the premises as part of the maintenance the data on that medium must be made unavailable for access by the appropriate process (refer to Trust's removable media policy).

### **Secure disposal of equipment**

All redundant ICT equipment must be disposed of according to Trust and national standards

### **Power Supplies**

It is the policy of the Trust to protect critical equipment (e.g. clinical and corporate systems) from power failure. A suitable supply as dictated by manufacturers' specification will be available and equipment in the computer room will have the benefit of the use of UPS (uninterruptible power supply) equipment.

Telecommunications equipment provided by telecommunications companies and other third parties will be installed underground, and terminated in a locked cabinet, and as a consequence is protected from unauthorised interception.

### **Equipment Maintenance**

Ongoing maintenance of computer equipment will normally be the subject of a maintenance agreement. However under certain circumstances it may be better value for money to replace equipment rather than continue to maintain. Under these circumstances the CDO will satisfy him/herself that any decision of this type will be to the benefit of the Trust.



## **13.0 COMPUTER AND NETWORK OPERATIONS**

Responsibilities and procedures for the management and operation of all computers and networks must be established and supported by appropriate operating instructions.

Access to the Trust's ICT facilities by third parties must be controlled

### **Network Management**

The Trust is required to conform to the NHS wide Networking Security Policy. The responsibility for ensuring that the Code of Connection continues to be met lies with the Chief Executive of the Trust, who delegates the task to the CDO who is the Trust's IT Security Officer. The Trust recognises that management of the NHS networking infrastructure reserves the right to disconnect the Trust if it is the offending organisation when a security breach occurs relating to data networking policy and the code of connection.

The Trust's data network has been designed to establish a secure networking infrastructure, that will support secure data transfer required by the Trust and fits into the secure infrastructure programme of the NHS.

The Trust recognises that the NHS wide networking security policy "seeks to provide a consistent approach to the security of networking services by ensuring that NHS information

- is not disclosed to unauthorised personnel
- is used only for the purpose for which it is intended
- has not been modified, either accidentally or maliciously
- is presented in the correct sequence for messaging applications
- is available when required".

Recognition of the Trust within the NHS wide security policy comes with the ability to certify that the Code of Connection Rules of the NHS wide networking programme are in place. This is a requirement in order to be able to connect any system or local network to the NHS wide networking infrastructure.

### **Health and Social Care Network**

The Health and Social Care Network (HSCN) is the new data network for health and care organisations which replaced N3. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly and efficiently.

From 31 March 2017, N3 network connectivity and existing contract arrangements moved onto the Transition Network. Organisations' N3 connectivity will continue to be supported through the Transition Network and full HSCN services are now available from a number of HSCN compliant suppliers. To exit Transition Network services and migrate to the HSCN, organisations' will need to start the procurement of new HSCN network services.

Health and care providers will be able to buy network connectivity from multiple suppliers in a competitive market place. To find out more visit our HSCN procurement section.

## **The HSCN Connection Agreement**

The Connection Agreement replaced the N3 Information Governance Statement of Compliance (IGSoC). In doing this, the arrangements for being able to use HSCN have been separated from those relating to accessing data or systems available on HSCN.

Every organisation that wishes to use HSCN must complete a Connection Agreement. By 'use HSCN', we mean 'send or receive data across HSCN'. Signing this agreement will mean that your organisation is ready to be connected to the HSCN once you've identified an HSCN supplier.

The HSCN Connection Agreement is organisation-centric: each organisation must sign just one Connection Agreement no matter how many locations or HSCN connections they have or use.

See a copy of the HSCN Connection Agreement. Please note this downloadable copy is for information purposes only. To sign the HSCN Connection Agreement for your organisation please see the Connecting to HSCN page.

The Trust will maintain action plans to ensure compliance with current and future standards

## **14.0 SECURITY INCIDENT MANAGEMENT**

There must be a formal procedure for reporting security incidents. Statistics on usual incidents must be gathered and all unusual security incidents must be investigated.

### **Security Incidents**

An information governance security incident is one, which can be defined as having resulted in:

- the disclosure of confidential information to an unauthorised individual
- the integrity of the data or the system being put at risk • the availability of the data or the system being put at risk
- An adverse impact, e.g.
  - Embarrassment to the Trust.
  - threat to personal safety or privacy
  - legal obligation or penalty
  - financial loss
  - disruption of activities

Incidents or information indicating a suspected or actual security breach must be reported to the immediate line manager and a Datix incident report submitted. All confidentiality incidents are screened on a daily basis and appropriate action including escalation or investigation undertaken where necessary. This will include reporting via the Data Security & Protection Toolkit to the Information Commissioner where the relevant threshold is met.

Refer to the Trust's Incident Policy for detailed information on the management of confidentiality breaches.

### **Access to Information**

There may be occasions when it is necessary to access information created or held by individual's on Trust's IT systems, resources and media for example when a person is away from the office for an extended period, on holiday or left the organisation. The reasons for accessing an individual's information are to action:

- Subject access requests under the data protection law
- Freedom of Information requests
- Evidence in legal proceedings
- Evidence in a criminal investigation
- A line of business enquiry
- Evidence in support of disciplinary action

Where it is not possible to seek the consent of the member of staff whose information needs to be accessed, the procedure for gaining access is:

- The appropriate line manager must complete the relevant access request form and obtain the necessary authorisations (Form C, Internet and Email usage policy)
- Submit the request to the Associate Director of Information Governance
- To ensure appropriate checks are made with Human Resources prior to release of Information
- Access is gained in the presence of a nominated IM&T staff member with a suitable witness where appropriate
- A record is made of the reasons for accessing the mailbox/information together with the names of the people who were present (By the Head of ICT Services)
- The person whose mailbox/information was accessed will be informed - where required/possible/appropriate – via receiving a copy of the relevant forms.

## **15.0 SYSTEM PLANNING AND PROCUREMENT**

Procurement procedures must encompass security aspects. All security requirements must be identified at the requirements phase of a project and included in the business case.

### **Procurement**

Procurement procedures must ensure that

- hardware or software changes which may affect network management and properly reviewed and approved
- mandatory and desirable security requirements are included in procurement specifications
- the IM&T security officer is consulted to ensure that the selected hardware and/or software will meet security requirements

Contracts must not be awarded until the security aspects are met.

Procurement procedures must consider the implications on disaster recovery plans in terms of compatibility with the existing plans.

### **Security requirements specification**

The necessary security requirements must be built into the project plan and progress must not be made without these included in the plan.

### **System changes**

All changes must follow Prince 2 project management methodology, and change control, with all security measures fully considered. All system changes must be fully tested, and assigned a system owner prior to sign off.

## **16.0 PROTECTION FROM MALICIOUS SOFTWARE**

Precautions are required to prevent and detect the introduction of malicious software. All managers and staff must be alert to the dangers of malicious software. IM&T staff must, where appropriate, introduce special measures to prevent or detect the introduction of viruses on PCs.

### **Procurement and licensing controls**

The Trust requires that all software used within the organisation is appropriately licensed and that no unlicensed software is used. The use of such software is prohibited. All software must be purchased through the IM&T department, following the IM&T purchasing procedure. This software will then be entered onto the inventory of approved software. Technically, the installation of software is only possible by authorised IM&T staff, and it will not be possible for staff to install software on their Trust PC.

### **Procedures must be in place to minimise the risk of the introduction of viruses.**

As part of this, users will be briefed:

- On the dangers of malicious software.
- Virus checking of all computer media either entering or leaving Trust premises.
- Checking all data or software imported or exported via networks.
- Ensuring appropriate backup procedures are in place and used.

- Ensuring that only officially provided and approved software is loaded onto PCs and servers.
- Ensuring that PCs are regularly checked for viruses.
- Regularly updating virus-checking software.
- The use of centrally controlled, regularly updated anti-virus software.

Procedures for checking and disinfecting any machine suspected of holding any malicious software must be established.

- Immediate virus checking of all other possibly infected machines isolating the machine immediately
- Preventing the use of the infected machine again until its reuse has been agreed by the Assistant Director for ICT
- Checking all software and data on the machine for the presence of viruses

## **17.0 HOUSEKEEPING**

Procedures must be established for backing up data, logging events and faults and where appropriate for monitoring the equipment environment. Operating procedures must protect media, data and systems documentation from damage, theft and unauthorised access.

### **Data back-up**

The Trust's data must be protected by clearly defined and controlled back up procedures, which will generate data for archiving and contingency recovery purposes.

Archived and recovery data must be accorded the same security as live data. This is also addressed under the Trust's business continuity plans.

## **18.0 DATA AND SOFTWARE EXCHANGE AND STORAGE**

Exchange of data and software between organisations must be controlled to prevent loss, modification or misuse of data. Storage before, during and after transfer must be secure.

Appendix G sets out NHS standards on use and management of Laptops within the NHS and these will be implemented across the Trust

### **Security of media in transport and storage**

The Associate Director of Information Governance will maintain a separate register of allowed bulk transfers of electronic person identifiable and sensitive data. All current and new bulk transfers are subject to the following:

**NO** person identifiable or sensitive information e.g. about service users, staff or carers, must be stored or transported on removable media such as CDs, floppy discs, DVDs, laptops or memory sticks unless:

- The data is **ENTIRELY** anonymous

Or

- The data is securely encrypted (including strong pass phrase protection to the Trust standards as defined in the Trust's Network, Internet and Email usage policy) • **and** there is a legitimate business or healthcare purpose for doing so;
- **and** your clinical director or borough director has expressly approved this
- **and** it has been authorized by the Trust's Head of Information Governance

### **Secure Storage**

Staff must **NEVER** store person identifiable or sensitive information on laptops or computer hard discs (usually your C Drive).

Where there is any doubt about the security of data held on any type of media, staff must seek immediate advice from the Information Governance team and ensure removable media and devices are securely stored in a locked cabinet, drawer or safe.

### **Couriers**

Reliable and approved couriers must be used at all times.

Where necessary special measures must be adopted to protect sensitive information from unauthorised disclosure (e.g. locked or sealable containers). In particular:

- Courier services must be approved by senior management as safe to handle confidential data
- All data/media for dispatch must be held in sealed envelopes or containers
- Appropriate tracking controls must be used to verify the safe dispatch, transit/delivery and (where appropriate) return of paper/media

### **Security of Email**

When using the E-Mail system staff must be particularly aware of:

- vulnerability to unauthorized interception or modification
- vulnerability to incorrect addressing
- publication of directory entries
- remote access to the E-Mail system and accounts Consideration must also be given to:
- the need to exclude sensitive information from the system

- The exclusion of third parties from E-Mail.

The transfer of personal or staff/patient confidential information via email requires assurance of the security of the route used, and encryption or anonymisation of data in line with national standards if this cannot be assured.

Please refer to the Trust's separate Network, Internet and Email policy for further information on the standards to apply.

## **19.0 GENERAL PRINCIPLES RELATING TO PATIENT/PERSON IDENTIFIABLE INFORMATION**

Organisations must restrict access to identifiable patient/person information to those authorized to see it. Only those users, who as a result of their tasks require access to person identifiable health data, must be allowed to access such data. Where possible staff/patient data must be anonymised.

### **Identifiable patient information**

The number and type of health related data items that could allow identification of an individual must be reduced to the minimum essential for the purpose if not anonymised.

### **Access limitations principles**

Authority to access identifiable patient information must be in accordance with the guidance in 'The Protection and Use of Patient Information', the Caldicott guidelines and under the "Data Protection Act".

There will be Trust arrangements for ensuring that patients are personally made aware of the purposes to which information about them may be put, as well as ways in which they can exercise choice.

### **Sharing patient/person information**

Identifiable patient/person information must not be shared with people who are not authorised to see it and recorded / tracked delivery must be used when sending original documents containing personal identifiable information via post. Original documents are official documentation issued by a government agency such as birth certificate, V5 etc. that cannot be replaced without going through a formal process. Photocopies do not fall into this category as another copy can be made from the original.

## **20.0 CONSENT**

Individuals will be fully informed regarding the information that is held about them and its intended use and when necessary, their consent sought for such use. This is in accordance with data protection law

## **Guidance on Consent-seeking**

To support staff, the Trust will put in place procedures that give clear guidance on:

- The need to seek consent and the consequences of not doing so;
- Who is trained to seek consent and how their involvement must be initiated.
- Who is able to take a decision on behalf of another person;
- The circumstances under which information may be disclosed without consent;
- Who can authorise the disclosure of information without consent and how this authority must be requested;
- The records which must be kept of this process;
- The procedures for recording and storing consent to share information;
- The procedures for recording limitations of consent to share;
- The procedures to be followed when consent is limited;

## **Obtaining consent**

The Trust recognises the need to handle consent seeking in as sensitive a manner as possible. Consent is not normally required for direct care purposes. Where consent is required this will be recorded on the relevant clinical system

Consent for non-direct care purposes will be sought at the earliest opportunity and subsequently at regular intervals. This must be at the first contact with the person concerned unless the individual is unable, at that time, to fully comprehend the implications or make an informed judgement.

Where a person does not have the capacity to make an informed decision but another person has authority to act as their guardian and take decisions on their behalf, then this situation must be explained to that person.

In order to ensure that consent to the sharing of personal information is informed, the Trust will have available, material that explains:

- The rights of individuals under the Data Protection Act 2018 and GDPR, particularly in relation to sensitive information;
- Details of the procedures in place to enable clients/patients to access their records
- Details of the procedures that may have to be initiated when a member of staff suspects that a patient has been or is at risk of abuse. These procedures must include details of whom information will be shared with at each stage, what information will be shared and how the information will be used.
- Details of the circumstances under which information may be shared without consent and the procedures which will be followed



- Details of the complaints procedures to follow in the event that the individual concerned believes information about them has been inappropriately disclosed.
- Details of how the information they provide will be recorded, stored and the length of time it will be retained both by the point of contact agency and the agencies to whom they may disclose that information.
- Details of the length of time for which consent to particular disclosures is valid

### **Recording consent**

Consent will be recorded on the relevant clinical system by which an individual or their guardian can record whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure.

Individuals must be able to prescribe, in respect of all information held by the Trust

- Which organisations they give permission for information to be, or not to be, shared with
- What information known to the Trust can be shared and what information must remain confidential

Consent to disclosure of personal information for a particular purpose, will be limited to a period to be specified by the individual or guardian, unless the individual concerned withdraws consent in the interim period.

The Trust will not seek consent to share information for direct care of a service user as explained in the leaflet “Your Records and You”, unless the service user specifically asks otherwise.

### **Checking for consent**

An individual’s record must always be checked before personal information is disclosed to another organisation.

Particular care must be taken before sensitive information is released. Special categories of information must only be released if their disclosure is vital to the case and explicit consent has been given to its release for that purpose, unless it is for direct care as explained above.

## **21.0 LOCAL POLICY**

Using the national guidelines published in “The Protection and Use of Patient Information”, the Trust has established its own Confidentiality Code of Conduct for identifiable patient information. This will be: -

- drawn to the attention of all staff,
- drawn to the attention of other bodies providing or working in conjunction with the Trust (e.g. GPs, CCGs, CSU, Social Care, etc) and, where necessary, discussed or agreed with them.

- Subject to monitoring and audit.
- Screen Savers are implemented on all Trust PCs
- A “clear desk” policy shall be in place to ensure sensitive information is locked away/secured at close of business

## **22.0 SHARING OF PERSONALLY IDENTIFIABLE INFORMATION**

**Objective:** To provide a framework for the secure and confidential sharing of information between organisations to enable them to meet the needs of patients for care, protection and support (and staff).

The exchange of information must conform to agreed protocols, including in disclosure in line with statutory responsibilities.

### **Protocols for sharing information**

Protocols for sharing information will be developed with all other NHS and external bodies with whom it can be reasonably anticipated that information may need to be shared. These protocols will permit the Trust’s Data Controller to monitor and audit the use to which transferred data is placed.

When disclosing information about individual service users, staff must indicate to what extent this information is current, is factual or an expression of opinion and whether it has been confirmed as correct by the individual.

### **Risk of prosecution**

Passing information without consent places both individual staff members and the Trust at risk of prosecution. If there is no lawful basis for disclosing information without consent, there is also the risk of a compensation order under the Data Protection Act, or damages for breach of confidence/breach of the Human Rights Act - Article 8 rights.

The disclosure of personal information without consent must be justifiable on statutory grounds and meet some conditions of the Data Protection Act/GDPR legislation.

A record of the disclosure will be made in the service user’s case file and the service user must be informed if they have the capacity to understand

Current facilities for controlling access to individual data items on computer systems and current arrangements for maintaining and storing paper-based client files, are such that access to a particular level of information cannot always be limited to those for whom permission has been given. Direct access by persons outside the Trust to the Trust’s computer systems cannot, therefore, be justified unless a third party access agreement is in place. .

The Associate Director of Information Governance will regularly monitor the Trust’s procedures for passing information to another organisation.

## **23.0 TRANSFER OF INFORMATION**

It is essential that requests for information about particular individuals be accompanied by sufficient personal information to ensure that the person can be clearly identified. In the absence of a common identifier, the name, address and date of birth of the data subject must accompany requests for information wherever possible.

### **Electronic transfer of personal information**

This will only be permitted on a person-to-person basis across secure networks or by encrypted and centrally authorised devices or media that are addressed or delivered directly to the intended recipient. Please refer to the Trust's separate Network, Internet and Email usage policy for further details on the transfer of person identifiable/sensitive/confidential data, encryption standards and limits to the use of portable/removable media.

### **Fax transfer of personal information**

Use of faxes must be avoided if possible but where necessary – follow the safe haven principles set out in Section 26.

### **Written/Oral/Face to face transfers of personal information**

The Trust has developed a separate Confidentiality Code of Conduct for transferring and sharing information verbally and in writing. Face-to-face and telephone transfers are also covered by this code.

It is recognised that in urgent cases, information about individuals, clients and/or patients may have to be requested or provided via the telephone.

Original written communications containing personal information must be transferred in a sealed envelope and addressed by name to the designated person within each organisation by means of recorded / tracked delivery. They must be marked "Personal and Confidential – to be opened by the recipient only". The designated person must be alerted to the despatch of such information and must make arrangements with their own organisation to ensure both that the envelope is delivered to them unopened and that it is received within the expected timescale.

### **Using personal information for purposes other than that agreed**

Organisations, to which Trust staff may disclose information, often fulfil a number of roles. In fulfilling one particular health/employment related role, they may be given privileged access to information about staff, a client or patient which they believe could assist them in one of their other roles, or be of wider interest to their organisation.

However, confidential information is disclosed only for the purpose specified at the time of disclosure. The Trust will make it a formal condition of disclosure that information provided must not be used for any other purpose without the consent both of the Trust's Data Controller and the data subject.

## **24.0 SHARING OF PSEUDONYMISED INFORMATION**

Pseudonymisation is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields makes the data record less identifiable while remaining suitable for data analysis and data processing.

The Informatics team would normally undertake this process, but there may be occasions where other staff such as performance managers are asked to undertake pseudonymisation. All staff would need to follow this process but the informatics team can provide support with this process.

In following this process the member of staff needs to ensure that they are aware of the difference between anonymised, pseudonymised and patient identifiable data and that they are sending data in the correct format. If unsure, they need to check this with the requester, the informatics team and seek advice from the information governance team

### **When to Use Pseudonymised data**

Pseudonymised data can be restored to its original state with the addition of information, which then allows individuals to be re-identified, while anonymized data can never be restored to its original state.

Examples of when the Trust may use or process pseudonymised data includes the National Patient Survey or Patient Audits for NHSE or Commissioners. This is where a third party is required to randomly select patients to be included in the survey or the audit but without seeing patient level detail.

It is important that when pseudonymising the data that there is a robust process in place to ensure that the information can be restored to its original state by the trust if required in order to carry out surveys and audits of the sampled cohort.

### **The De-Identification Process**

The process that the Trust follows is outlined below.

- a) Extract the data from the appropriate clinical system in line with the reporting requirements requested.
- b) Information should be provided in a CSV or Excel spreadsheet and should include a patient identifier. This can be the clinical system number or NHS number.
- c) In a spreadsheet, create two additional columns. Step d and e only apply when required pick random set of patient list
- d) In first column – title the first row as Random and in the second row first cell type the formula =Rand().
- e) Double click on the cell to fill in the column.
- f) In second Column – Title as System User Code on the first row.

- g) On the Second Row – You will need to create your pseudonymised naming convention.
- For example if you are doing a Mental Health Audit for year 18, use the NHS Organisation Code for the Trust which is RWK – so the System User Code will be MH18RWK000001.
  - You will need to ensure that you put enough digits to cover the full sample size. So you will need to know how many records are likely to be extracted. For the patient survey, six digits are used to be on the safe side.
- h) Double click on the cell to fill in the column.
- i) Ensure that the original document is saved in the appropriate folder.
- j) When sending the file ensures that, the patient identifiable information is removed and is sent securely to the recipient.
- k) If the information is to be used for sampling a cohort for audit purposes, on receipt of the sample use the original file to re-identify the patient details in order to provide the appropriate patient information to carry out the task required i.e. patient audit.
- l) Any data shared externally will be logged in the Pseudonymised log held by the informatics team on a shared drive.

## **Audit**

An annual audit is undertaken by the informatics team to ensure that the pseudonymisation process is followed correctly. Feedback is provided in an action plan as appropriate in order to address any action that needs to be taken.

This process is to be reviewed annually to ensure that it meets the needs of the Trust and any other changes that may need to be accommodated.

## **25.0 LEGISLATION AND GUIDANCE ON USING PERSON IDENTIFIABLE DATA**

**Objective:** To ensure that staff are familiar with their legal responsibilities.

The key legislation governing the protection and use of identifiable patient/client information (Personal Data) is the Data Protection Act 2018 (DPA 2018) and GDPR. The DPA does not apply to information relating to the deceased. .

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making and profiling.

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

### **Pre-requisites for the processing of any personal data**

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it.
- Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

### **Summary of the seven Caldicott principles**

- Principle 1: Do you have a justified purpose for using confidential information?
- Principle 2: Is it absolutely necessary to do so?
- Principle 3: Are you using the minimum information required?

- Principle 4: Are you allowing access to this information on a strict need-to-know basis only?
- Principle 5: Do you understand your responsibility and duty to the subject with regards to keeping their information secure and confidential?
- Principle 6: Do you understand the law and are you complying with the law before handling the confidential information?
- Principle 7: Do you understand that the duty to share information can be as important as the duty to protect confidentiality?

## **26.0 USER ACCESS CONTROL**

**Objective:** To restrict access to business information to authorized users.

Access to computer services and to data must be controlled on the basis of business requirements, which take account of policies for information dissemination and entitlement.

There must be formal procedures to control allocation of access rights to IM&T services. Special attention must be given to the control of allocation of privileged access rights, which allow users to override system controls.

Users must be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use and security of passwords and of user equipment.

### **NHS.net**

The Trust must conform to the code of connection for data

### **Planning access control permissions**

The Trust has adopted the following methodology to define access control permissions:

- Step 1 identifies the roles which may have a legitimate interest in information relevant to the subject of the protocol
- Step 2 defines levels of information that are relevant to the protocol. Different levels will reflect degrees of confidentiality. Confidentiality may be necessary either from a commercial/business perspective or from legal responsibilities to protect the confidentiality of service users.
- Step 3 sets out the reasons which may justify access to a particular level of information
- Step 4 produces a matrix showing the access available for each role to each level of information and notes the reason whereby that access is justified. Access to a particular level of information required is granted only in relation to the specified function, and its use for any other function which that person may fulfil, whether in the course of their employment or not, requires a separate approval from those responsible for controlling access to information originating from their organisation.

## **Documented access control**

The business requirements for access control must be defined and documented for each system. The documentation for each system must clearly define the access rights of each user or group of users

## **User registration**

There must be a formal documented user registration and de-registration procedure for access to systems. This must:

- check that the user has authorisation from the system owner
- check that the level is appropriate for the business purpose
- ensure that access is not given until the authorisation process is complete
- maintain a register of people registered to use a particular system
- assess access rights of users who change responsibilities and where necessary change to appropriate access levels
- Remove access rights of users leaving the Trust.

A process to review access rights must be established.

## **Special privilege management**

These are privileges normally allocated to the systems manager or systems administrator, which give access to routines, which expose the systems vulnerabilities of a system. The allocation of special privileges for network and other corporate systems must be controlled. An authorisation process must be in place which:

- identifies who must have special privileges
- can allocate and revoke special privileges on an ad hoc basis
- maintain a record of who has been allocated special privileges

## **User password management**

Users must be briefed on the importance of passwords and advised as to the appropriate ways of use. Passwords must be memorised by users and not written down

Passwords must not be displayed on screens as they are entered.

When allocated a new/temporary password for start-up use by the systems manager/administrator the user must immediately change it.

Password must ask for authentication by re-entering Passwords must consist of a minimum of 6 characters

Passwords must be changed on change of staff or staff resignation



Users must have their own passwords although under some circumstances where sharing of systems is necessary a separate password relating to the PC must be available

Passwords must not normally be written down.

Passwords must not relate to the system or the user although passwords must be easy to remember

Password must be changed regularly and changed where some form of compromise may be suspected

## **27.0 COMPUTER ACCESS CONTROL**

**Objective:** To prevent unauthorised computer access.

Access to computer facilities must be restricted to authorised users. Computer systems that serve multiple users must be capable of the following:

- identifying and verifying the identity and the location of each user
- recording successful and unsuccessful system accesses
- controlling the connection times of users

### **Terminal log on procedures**

Access to IM&T services must be via a secure log on process designed to minimise the opportunity for unauthorised access. The log on process must:

- not display system or application identifiers
- display a notice that the system must only be used by authorised users
- not provide log on help
- validate log on information after all data input
- limit unsuccessful attempts to access the system to 3
- on failure to log on due to too many attempts, register the attempt, force a time delay to the next series of attempts and disconnect the data link
- limit the time allowed to access - failure due to time must be regarded as a failure equivalent to failing after more than 3 attempts
- Display information about the last successful log on to offer checking by the authorised user.

### **User identifiers**

Each user must have a unique identifier giving no indication of the privilege level.

## **Inactive terminals**

Inactive terminals must time out to a screen saver after a specified period of time. All screen savers must be password protected. Users must ensure that PCs/terminals are logged off when leaving unattended.

## **28.0 APPLICATION ACCESS CONTROL**

**Objective:** To prevent unauthorized access to information held in computer systems

Logical access controls must restrict access to application systems and data to authorized users

Applications must: -

- control user access to data and application system function
- provide protection from unauthorized access to software capable of overriding application controls

### **Information access restriction**

Access to data must only be granted to staff that need to use the data to perform their job function.

Special arrangements must be available for emergency purposes (e.g. access to technical staff or engineers) where the password must be changed at the completion of the emergency activity.

All detected unauthorized attempts at access must be notified to the IM&T security officer

### **System utilities access restriction**

The use of systems utilities must be restricted and controlled. Control must be of the following type:

- password protection for system utilities
- segregation of system utilities from applications

Restriction of use to 'trusted' and authorized users

- logging of the users of the systems utilities and the levels of authorization

### **Control of access to program source libraries**

Strict control must be maintained as follows:

- program sources must not be held on operational systems
- programs under development must not be held on operational systems
- controls over access to program sources must be in place
- version management must be in operation to control the distribution of software • an audit log of access to program libraries must be maintained

## **29.0 DISPOSAL OF IM&T EQUIPMENT**

The ICT Department must ensure that all ICT equipment and media are disposed of in an appropriate and secure manner.

In adhering to the Data Protection Act and the IM&T Security Policy, the information that is stored on the hard drive of a computer must also be destroyed.

The following table is not an exhaustive list of all possible media types, but instead offers a representative sample of the most common forms of media currently in use. These media types also demonstrate the characteristics that determine the appropriate deletion or destruction methods required to assure data is non-retrievable.

<b>Media Type</b>	<b>Data Storage Mechanism</b>	<b>Suggested Removal Methods</b>
Hard Disk Drives	Non-volatile magnetic	Pattern wiping, Incineration
CDROM/DVD-R	Write once optical	Abrasion, Incineration
CD-RW/DVD-RW	Write many optical	Abrasion, Incineration
Magnetic Tape	Non-volatile magnetic	Degaussing, Incineration
Flash Disk Drives	Solid state	Pattern wiping, Physical destruction
Paper Based	-	Shredding, Incineration

The Assistant Director of ICT will maintain and publish a separate Disposal of IM&T Equipment policy and procedure to cover this.

- 

### **30.0 DATA VALIDATION**

Appropriate security controls including audit trails must be designed into application systems to prevent loss. Modification or misuse of data

#### **Input data validation**

Controls must be designed into systems so that:

- the integrity of data is maintained through the use of reference file data and cross checking and validation
- numbers of records, values etc can be checked through systems
- batch controls are included where appropriate

Rejected data must be output showing reason for rejection and returned to user for correction and completion.

A log must be kept of any notified losses or corruption in data.

#### **Data Encryption**

The Trust will maintain standards for use of data encryption techniques in line with NHS requirements and staff will be given and tools to enable use of encrypted email attachments provided where these are required for secure transmission of personal/sensitive information.

These will be published in a separate Network, Internet and email usage policy.

#### **Message Authentication**

Authentication techniques must be adopted where critical/confidential data is involved

### **31.0 BUSINESS CONTINUITY PLANNING**

**Objective:** To be able to maintain business activities after any unforeseen major failure or disaster

There must be a process to develop and maintain appropriate plans for the speedy restoration of critical business processes and services in the event of serious business interruptions.

Business continuity planning must include measures to limit the consequences of any threats that are realised and to provide a resumption of essential operations as soon as required.

#### **Business continuity planning process**

The planning process must include the following: -

- a formal documented assessment of how long users could manage without each computer system

a formal documented assessment of how critical each system is, including the implications of its loss

- identification and agreement of all responsibilities and emergency arrangements
- documentation of agreed procedures and processes
- a formal assessment of the resilience of the plans and how quickly continuity will be achieved
- Multiple copies of plans must be kept both on site and off site (e.g. at managers' homes)

### **Business continuity planning framework**

A framework must be in place with four components:

- emergency procedures describing the actions to be taken following an incident which will jeopardise business operations
- fall back procedures for both short term and long term loss which describe the actions to be taken to move essential business activities to alternative locations
- resumption procedures which describe the actions to be taken to return to normal full operations at the original site (e.g. Defined and controlled data backup procedures)
- a test schedule that specifies how and when the plan can be tested.

### **Testing and Updating business continuity plans**

A test schedule must be drawn up for each contingency plan.

Business continuity plans must be reviewed and updated as part of the IM&T strategy development process.

### **Responsibilities**

Each service area, team, ward or department is responsible for devising local coping strategies and contingency plans to deal with the loss or unavailability of IM&T assets or systems.

Local system managers, must ensure these arrangements are in place, effective and understood by all relevant staff – the priority for such work will be given to service critical systems

## **32.0 COMPLIANCE**

**Objective:** To comply with any statutory obligations

- 

All relevant statutory and contractual requirements must be explicitly defined and documented for each system. The controls, countermeasures and individual responsibilities to meet these requirements must be similarly defined and documented.

Advice on specific legal requirements must be sought from the Authority's advisors

### **Control of proprietary software copying**

No copyright material must be copied without the copyright owner's consent

### **Safeguarding of Organizational Records**

Guidelines on the retention, storage, handling and disposal of medical and other records and information must be maintained. These guidelines must be aimed at protecting essential records and information from loss, destruction and falsification.

### **Data Protection**

The Trust must confirm that the designated persons charged with ensuring that appropriate procedures are in place to meet the requirements of the Data Protection Act 2018 and GDPR are appropriately trained.

### **Prevention of misuse of IM&T facilities**

Employees of the Trust and any third party users must be informed that no access to systems is permitted unless formal authorization has been given. Failure to comply with this could be in breach of the Computer Misuse Act (1990), which identifies three criminal offences:

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

## **33.0 RISK ASSESSMENT**

**Objective:** To ensure that countermeasures are appropriate to risk, in compliance with NHS security policies and standards.

The security of IM&T systems must be regularly assessed. Risk assessments must be done against the appropriate security policies, and the technical platforms and IM&T facilities checked for compliance with the NHS IM&T Security Manual.

### **Compliance with security policy**

The Associate Director of Information Governance and the CDO must ensure that each system under the control of the Trust is subject to regular security risk assessments. The degree of detail of the risk assessment will depend on the value of the asset(s). All reports must remain confidential.

Risk Assessment can be broken down into four main functions:

- Identification of the assets,
- Evaluation of the impact of an adverse event (threat) on the assets,  
Assessment of the likelihood of the adverse event occurring,
- Identification of appropriate countermeasures to protect the asset and/or limit the damage caused by an event.

### **Countermeasures**

The IM&T security officer must:

- ensure that countermeasures are implemented sensibly, effectively and cost efficiently,
- regularly re-examine the Trust's use of any countermeasures and their continuing suitability and effectiveness.

A report must be produced following the examination.

## **34.0 SAFE HAVEN PRINCIPLES AND FAXES**

The Trust will maintain a list of Safe Haven fax machines in use.

To ensure secure transmission and receipt of faxes the following practice and principles will be followed. Faxes must only be used when there is no other means of communication.

- Ensure fax machines are sited in an area that is restricted to those who need to access the information
- An ideal is in a locked cupboard or room so that any faxes received out of hours are secure
- Pre-programme outgoing fax numbers to ensure there is no chance of dialling the wrong number. Always check the entered/displayed fax number before pressing "Send"
- Where possible do not use personal/identifiable information - use a number (such as NHS number)
- If it is very confidential/sensitive information, ensure someone is at the receiving end is waiting by the receiving fax machine, check the fax number with them and ask them to confirm receipt.
- Follow the guidance set out in information sharing protocols between you and any organisation sending and receiving information (Both this Trust and the recipient have a duty of confidentiality)
- Be aware of the law - common law of Confidentiality, Data Protection Act, Human Rights

- 
- Ensure staff have a confidentiality clause in their contract of employment
- Ensure only authorised staff handle confidential information
- Ensure you have the consent (or it is covered by law) for the sharing of information



- 

Safe havens also apply to telephone, mail, answer phones, conversations and any other way that confidential information is shared.

- Use available NHS safe haven telephone numbers as published via approved DoH web sites.

If in doubt staff must discuss action with their line manager or seek advice from the Information Governance team.

## **35.0 NETWORK SECURITY POLICY**

The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

### **• The policy**

- Sets out the organisation's policy for the protection of the confidentiality, integrity and availability of the network.
- Establishes the security responsibilities for network security. Provides reference to documentation relevant to this policy.

### **• Aim**

The aim of this policy is to ensure the security of ELFT's network. To do this the Trust will:

- Ensure Availability
- Preserve Integrity
- Protect the network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets.
- Preserve Confidentiality
- Protect assets against unauthorised disclosure.

### **• Network definition**

The network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables. The network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

### **• Scope of this Policy**

This policy applies to all networks within ELFT used for:

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images

- 

Printing or scanning non-clinical or clinical data or images

- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

### • **The Policy**

The overall Network Security Policy for ELFT is described below:

The ELFT information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, ELFT will undertake to the following:

- Protect all hardware, software and information assets under its control.

This will be achieved by implementing a set of well-balanced technical and non-technical measures.

- Provide both effective and cost-effective protection that is commensurate with the risks to its network assets.
- Implement the Network Security Policy in a consistent, timely and cost effective manner.
- Where relevant, ELFT will comply with:
  - Copyright, Designs & Patents Act 1988 Access to Health Records Act 1990 Computer Misuse Act 1990
  - The Data Protection Act 2018 GDPR
  - The Human Rights Act 1998
  - Electronic Communications Act 2000 Regulation of Investigatory Powers Act 2000 Freedom of Information Act 2000
  - Health & Social Care Act 2001
- ELFT will comply with other laws and legislation as appropriate.
- The policy must be approved by the Information Governance Steering Group

### • **Risk Assessment**

ELFT will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

- Physical & Environmental Security
  - Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment with controlled temperature and monitored power supply quality.

- Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- The Network Manager is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if s/he suspects the code has been compromised, or when required to do so by the Information Security Officer.
- Critical or sensitive network equipment will be protected from power supply failures.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.
- All visitors to secure network areas must be authorised by the Network Manager.
- All visitors to secure network areas must be made aware of network security requirements.
- All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
- The Network Manager will ensure that all relevant staff are made aware of procedures for visitors and those visitors are escorted, when necessary.

• **Access Control to Secure Network Areas**

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The Network Manager will maintain and periodically review a list of those with unsupervised access.

• **Access Control to the Network**

- Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- There must be a formal, documented user registration and de-registration procedure for access to the network.
- Departmental managers must approve user access.
- Access rights to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Security privileges (i.e. 'superuser' or network administrator rights) to the network will be allocated on the requirements of the user's job, rather than on a status basis.
- Access will not be granted until the ICT department registers a user.
- All users to the network will have their own individual user identification and password.
- Users are responsible for ensuring their password is kept secret (see User Responsibilities).
- User access rights will be immediately removed or reviewed for those users who have left the Trust or changed jobs, following notification from the HR dept or line manager.

### • **Third Party Access Control to the Network**

- Third party access to the network will be based on a formal contract that satisfies all necessary NHS security conditions.
- All third party access to the network must be logged.

### • **External Network Connections**

- Ensure that all connections to external networks and systems have documented and approved System Security Policies.
- Ensure that all connections to external networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance.
- The Information Security Officer must approve all connections to external networks and systems before they commence operation.

### • **Maintenance Contracts**

The Network Development Manager will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment. All contract details will constitute part of the Information Department's Asset register.

### • **Data and Software Exchange**

Formal agreements for the exchange of data and software between organisations must be established and approved by the head of Information Governance.

### • **Fault Logging**

The Network Manager is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

### • **Network Operating Procedures**

- Documented operating procedures must be prepared for the operation of the network, to ensure its correct, secure operation.
- Changes to operating procedures must be authorised by the Associate Director for ICT

### • **Data Backup and Restoration**

- The Network Development Manager is responsible for ensuring that backup copies of network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant staff.
- All backup tapes will be stored securely and a copy will be stored off-site.

- 

- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.

Users are responsible for ensuring that they backup their own data to the network server.

- **User Responsibilities, Awareness & Training**

- The Trust will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
- All users of the network must be made aware of the contents and implications of the Network Security Policy.
- Irresponsible or improper actions by users may result in disciplinary action(s).

- **Accreditation of Network Systems**

Ensure that the network is approved by the Information Security Officer before it commences operation. The Information Security Officer is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation.

- **Security Audits**

The Associate Director of Information Governance will require checks on, or an audit of, actual implementations based on approved security policies.

- **Malicious Software**

Ensure that measures are in place to detect and protect the network from viruses and other malicious software.

- **Secure Disposal or Re-use of Equipment**

Ensure that where equipment is being disposed of the Trust policy on disposal of ICT equipment is followed.

- **System Change Control**

- Ensure that the Network Manager reviews changes to the security of the network. All such changes must be reviewed and approved by the Associate Director for ICT. The Network Development Manager is responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.
- The Assistant Director for ICT may require checks on, or an assessment of the actual implementation based on the proposed changes.
- The Assistant Director for ICT is responsible for ensuring that selected hardware or software meets agreed security standards.

- 

- As part of acceptance testing of all new network systems, the Assistant Director for ICT will attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.

Testing facilities will be used for all new network systems. Development and operational facilities will be separated.

- **Security Monitoring**

Ensure that the network is monitored for potential security breaches. All monitoring will comply with current legislation.

- **Reporting Security Incidents & Weaknesses**

All potential security breaches must be investigated and reported. Security incidents and weaknesses must be reported in accordance with the requirements of the organisation's incident reporting procedure.

- **System Configuration Management**

Ensure that there is an effective configuration management system for the network.

- Business Continuity & Disaster Recovery Plans
- Ensure that business continuity plans and disaster recovery plans are produced for the network.
- The plans must be reviewed by the Information Security Officer and tested on a regular basis.

- **Unattended Equipment and Clear Screen**

- Users must ensure that they protect the network from unauthorised access.

They must log off the network when finished working.

- The Trust operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.
- Users failing to comply will be subject to action which may in some circumstances result in disciplinary procedures.

- **Security Responsibilities**

The Chief Executive has delegated the overall security responsibility for security, policy and implementation to the Associate Director of Information Governance for information management security and the Chief Digital Officer for IT security.

- **Network Manager's Responsibilities**

- To produce and implement effective security countermeasures.

- 

- Produce all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the Network Security Policy.
- All such documentation will be included in the IM&T Department's Asset register.

Ensuring that access to the organisation's network is limited to those who have the necessary authority and clearance.

- **Information Security Officer Responsibilities**

- Acting as a central point of contact on information security within the organisation, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.
- Produce organisational standards, procedures and guidance on Information Security matters for approval by the Information Governance Steering Group.
- Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
- Ensuring that appropriate Data Protection Act notifications are maintained for information stored on the network.
- Advising users of information systems, applications and networks of their responsibilities under the Data Protection Act, including Subject Access.
- Encouraging, monitoring and checking compliance with the Data Protection Act.
- Liaising with external organisations regarding Data Protection Act matters.
- Promoting awareness and providing guidance and advice related to the Data Protection Act as it applies within the Trust.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Representing the organisation on internal and external committees that relate to IT security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally.

- 
- Providing advice and guidance to development teams to ensure that the policy is complied with.
- Approving system security policies for the infrastructure and common services.
- Approving tested systems and agreeing rollout plans.
- Providing a central point of contact on IT security issues.
- Providing advice and guidance on:
  - Policy Compliance
  - Incident Investigation
  - IT Security Awareness
  - IT Security Training
  - IT Systems Accreditation
  - Security of External Service Provision
  - Contingency Planning for IT systems
- Contacting the Information Security Manager when:
- Incidents or alerts have been reported that may affect the organisation's systems, applications or networks.
- Proposals have been made to connect the organisation's systems, applications or networks to systems, applications or networks that are operated by external organisations.
- Passing on the advice of external sources/authorities on IT security matters.
- **Line Manager's Responsibilities**
  - Ensuring the security of the network, that is information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
  - Ensuring that their staff are made aware of their security responsibilities.
  - Ensuring that their staff have had suitable security training.
- **General Responsibilities**
  - All personnel or agents acting for the organisation have a duty to:
  - Safeguard hardware, software and information in their care.
  - Prevent the introduction of malicious software on the organisation's IT systems.
  - Report on any suspected or actual breaches in security.



- 

- **Guidelines**

Detailed advice on how to determine and implement an appropriate level of security is available from the Information Security Officer

**Appendix A**

**Suggested minimum format for [location] Asset Register**

Responsibility for security control of assets					
Name of asset	Owner	Site	System name	Access control	What type of access the user is allowed
1					
2					
3					
3					
4					
5					

**TO BE COMPLETED AND MAINTAINED BY INFORMATION DIRECTORATE**

## **Appendix B Information Assets – Requirements for Classification**

An owner needs to be identified for each logical or physical set of data:-

1. Name of the system - logical or physical set of data The data owner will be responsible for the following
2. How the data can be used
3. Who can access the data and what type of access each user is allowed? by individual? or job title?
4. Determine the classification or sensitivity level of the data
5. Review the classification and notify the Associate Director of Information Governance
6. Approving appropriate security protection for the data
7. Ensure compliance with security controls
8. Ensure compliance with the DPA and other relevant legislation Consistency across systems is required

Labelling of sensitive data is required Sensitivity levels may change over time.

9. Importance of asset to service provision (Service Critical/Important/Non Critical)
10. Classification of 'owner' for:
  - central systems
  - distributed assets
  - departmental assets

## **Appendix C Summary of Objectives**

The purpose of the Trust's policy, as described above, is implemented through a series of objectives. The actions resulting from the task of meeting these individual objectives are the manner in which the Trust's security policy is appropriately enforced.

The objectives for the Trust are:-

### **Objective 1 Management of Security**

To manage information security within the Trust.

### **Objective 2 Job Definitions and Resourcing**

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

To ensure that users are aware of information security threats and concerns, and are equipped to support the Trust's security policy in the course of their normal work.

### **Objective 3 Responsibility for Security Control of Assets**

To ensure that the responsibility for the security of all IM&T assets is assigned.

### **Objective 4 Access Control to Secure Areas**

To prevent unauthorised access, damage and interference to IM&T services.

### **Objective 5 Equipment security**

To prevent loss, damage or compromise of assets and interruption to business activities.

### **Objective 6 Computer and Network Operations**

To ensure the correct and secure operation of computer and network facilities.

### **Objective 7 Security Incident Management**

To ensure that information security breaches are detected, reported and investigated.

### **Objective 8 System Planning, Procurement and Acceptance**

To ensure that security is built into systems.

### **Objective 9 Protection from Malicious Software**

To safeguard the integrity of software and data.

**Objective 10 Housekeeping**

To maintain the integrity and availability of IM&T services and to prevent damage to assets.

**Objective 11 Data and Software Exchange**

To prevent loss, modification or misuse of data.

**Objective 12 General Principles Related Patient Information**

To restrict access to identifiable patient or personal information to those authorized to see it.

**Objective 13 Collecting Personally Identifiable Information**

To assist in conforming with the law in respect of the processing of personally identifiable information.

**Objective 14 Sharing Of Personally Identifiable Information**

To provide a framework for the secure and confidential sharing of information between organisations to enable them to meet the needs of patients for care, protection and support. (and for staff in employment and delivering that care)

**Objective 15 Key Legislation And Guidance On Using Personally Identifiable Data To**

ensure that staff are familiar with their legal responsibilities.

**Objective 16 User Access Control**

To restrict access to business information to authorized users.

**Objective 17 Computer Access Control**

To prevent unauthorized computer access.

**Objective 18 Application Access Control**

To prevent unauthorized access to information held in computer systems.

**Objective 19 Data Validation**

To prevent loss, modification or misuse of data.

**Objective 20 Business Continuity Planning**

To be able to maintain essential business activities after any unforeseen major failure or disaster.

**Objective 21 Compliance**

To comply with any statutory obligations.

## **Objective 22 Risk Assessment**

To ensure that countermeasures are appropriate to risk in compliance with NHS security policies and standards.

**Appendix D - Compliance statement and pro-forma required from third parties**



**AGREEMENT WITH EAST LONDON NHS FOUNDATION**

**TO ABIDE BY TRUST CONFIDENTIALITY, INFORMATION AND IM&T SECURITY REQUIREMENTS**

**I have read and fully understood the Trust's Information Governance and IM&T Security Policy and agree that staff, services provided and transactions carried out for the Trust under the contract comply with the requirements set out therein.**

The contractor will

- Ensure the safe and proper handling, storage and transportation of information and records accessed or available to the contractor either as part of their work or because they are working on Trust premises or with Trust staff.
- Note that this agreement is required in addition to any reference to security and confidentiality that there may be in the support contract.
- Ensure that all employees and sub-contractors working for them on this Trust's premises, information, IT systems and records are aware of and agree to comply with the security and confidentiality requirements set out in the attached Policy.
- Indemnify the Trust against a breach by themselves, employees or any third party subcontractor

<b>Name of Contractor</b>	
<b>Contract Description</b>	
<b>Date of Agreement/contract</b>	
<b>Expiry date – where applicable</b>	
<b>Name of Contractor's Data Protection Officer or officer with authority</b>	
<b>Position Held</b>	
<b>Signature</b>	
<b>Date</b>	

**(Signed copies required and to be retained by both Contractor and Trust)**

## **Appendix E – The connection of unsecured devices to the Trust network**

The connection of any unsecured (non-firewalled) device to trust PC's or network equipment is strictly prohibited in accordance with NHS Security policies. The following list is meant as a guide and is not exhaustive. Any non-standard IT equipment would need to be approved by the Information Directorate (Head of ICT) before purchase and connection to the Trust network.

### **Connection of the following devices (or similar) to the Trust network is prohibited:**

- Mobile phones
- Smart phones
- Non trust Blackberries
- Non-approved PDA's
- Personal laptops\computer\networking equipment
- Portable gaming devices
- Portable music players
- Photocopiers
- Multi-function devices (fax\photocopier\printer etc.)
- Any device that includes wireless networking
- Any other non-approved device

A comprehensive list of approved devices will be maintained is in the Trust IM&T Services Purchasing and Procurement Policy and Procedure, which will be made available on the Trust Intranet.

The Trust will develop and/or procure tools to monitor and restrict the connection and use of such devices, and will issue instructions to staff as technologies evolve and as appropriate controls are introduced.



## **Appendix F - General Management of Laptops**

A Local Laptop Manager (LLM) must be appointed to take overall responsibility for the management of each NHS organisation's laptop estate.

### **Registration**

- All laptops used for NHS business or holding NHS information must be uniquely identified and registered in the organisation's records as information governance security relevant items.

### **Accountability**

- Responsibility for the security of an NHS organisation's registered laptops and their data must be assigned to individuals and tracked alongside the employment status of those individuals.

### **Management of laptop security functionality**

- The installation and configuration of laptop security functionality, including access control, encryption and tamper resistance must be undertaken by appropriately trained staff.

### **User training and awareness**

- Users of laptops must be given appropriate training and instruction in the use of the laptop and its security functionality. This must include their responsibility for safeguarding the laptop and their obligation to comply with relevant information governance security procedures of the organisation.

### **Security accreditation**

- The local IT Security manager or equivalent must regularly review the NHS organisation's laptop estate to ensure that they continue to meet these requirements and that the residual level of risk from their use is acceptable.

### **Authorization**

- Regardless of a laptop's ownership, the use of any equipment outside an NHS organisation's business premises for the processing of NHS information must be authorized by the relevant Director or Head of Department. Where the processing of NHS patient information is proposed on laptop devices additional authorization must be obtained from the organisation's Caldicott Guardian.

### **Physical**

- It is recommended that laptops, even when protected by disk encryption, must not be left in the care of any person who is not trusted to protect the information it contains.

### **Availability**

- Continued availability of laptops, for operational reasons and because of the costs of replacement, will mean that consistent standards of physical and procedural protection will be

required for all laptops used by the NHS organisation. These must be defined within local information governance policy, and relevant staff and contractors made aware.

### **Remote Access**

- Remote access from a laptop to NHS information systems must be achieved in accordance with the organisation's NHS IG Statement of Compliance, NHS IG guidance, and any defined requirements for the protection or use of the NHS information service(s) concerned.

### **Data Storage and Use**

- Sensitive data, including that relating to patients, stored on an NHS laptop must be kept to the minimum required for its effective business use in order to minimise the risks and impacts must a breach occur.

### **Incident Reporting**

- Loss of NHS laptops must be reported in accordance with the information governance incident management arrangements implemented locally. Details of these arrangements must be provided to all laptop users.

### **Secure Disposal and Reuse**

- Data stored on NHS laptops must be securely erased before the laptop is reassigned for another purpose or disposed of when redundant. Failure to securely erase data may result in that data being available to the new owner/user of the laptop. NHS information governance guidance is available from NHS Connecting for Health for this purpose.