NHS
East London
NHS Foundation Trust

Information Governance and Information Management and Technology Security Policy

Version number :	5.9
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	IGSG Chair’s Action
Ratified by:	IGSG Chair’s Action
Date ratified:	28 May 2024
Name of originator/author:	Head of Information Governance
Executive Director lead :	Chief Quality Officer
Implementation Date :	May 2024
Last Review Date	May 2024
Next Review date:	May 2027

Services	Applicable
Trustwide	X
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
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
5.9	May 2024		Draft	Annual Review and Update.

Contents

Appendices

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 Information Management & Technology (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, and 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 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 you 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 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 be 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 8 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.

Media Type	**Data Storage Mechanism**	**Suggested Removal Methods**
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 Cyber Security Specialist/Support 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

NHS
East London
NHS Foundation Trust

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

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

(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 securityrelevant 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.

East London
NHS Foundation Trust

Access to Records Policy

Version number:	1.8
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	Information Governance Steering Group
Date approved	28th August 2024
Ratified by:	Quality Committee
Date ratified:	27th November 2024.
Name of originator/author:	Information Governance Manager – Bedfordshire & Luton and London
Executive Director lead:	Chief Quality Officer
Implementation Date:	November 2024
Last Review Date	August 2024
Next Review date:	August 2027

Services	Applicable
Trust wide	X
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0	14.10.11	Head of Information Governance	Final	New policy incorporating previous Access to Health Records policy, Access to Non Health Records policy and Newham PCT Information Disclosure Guidelines
1.1	23.04.13	Head of Information Governance	Final	Section 9.6 (Fees) strengthened
1.2	15.01.15	Information Governance Assets Manager	Final	Minor amendments for consistency of job role titles and addition of monitoring, reference and additional documents sections in line with Trust Policy template
1.3	08.11.18	Information Rights Manager		Policy reviewed to incorporate the GDPR/Data Protection Act 2018. Also some procedural change regarding SAR to HR.
1.4	02.07.19	Information Governance Manager		Policy reviewed to incorporate the ICO audit actions (updating third parties about inaccuracies corrected; procedure for deleting information; acknowledge verbal requests as valid option).
1.5	20.09.21	Information Governance Manager		Policy reviewed to incorporate Transfer of Care requests from other NHS organisations, procedure reviewed due to staff changes
1.6	12.04.22	Information Governance Manager – Information Rights		Policy reviewed to reflect The Data Protection Act 2018 and remove references to GDPR. Additional references made where requests for information from other agencies have been received. Rights to rectification and erasure have been expanded on to include where these requests should go to. Reference to responding to an Access to Health Records Request in one month has been changed to 21

				calendar days.
1.7	19.06.23	Data Protection Officer		Staff subject access requests process strengthened
1.8	13.08.24	Information Governance Managers		Policy reviewed to reflect new team structure (remove references to Information Rights Manager and include new Senior Information Governance Managers (Systems and Compliance), and London & Bedfordshire & Luton Information Governance Manager roles). Procedure for processing CCTV footage requests has also been clarified.

Contents

Paragraph **Page**

1.0 Introduction

Individuals have a right to apply for access to their personal information, and in some cases, information held about other people. This policy ensures individuals can exercise this right.

2.0 Purpose

This policy sets out who may apply for access, their rights, relevant legislation, responsibilities and the subject access requests handling process. This policy will be on the Trust's intranet under Information Governance.

3.0 Duties

The Associate Director of Information Governance (who is the Data Protection Officer) is responsible for protecting the confidentiality of a patient and service -user information and enabling appropriate information -sharing and has overall responsibility for ensuring adherence to this policy. A Data Protection Officer is a legal requirement under Section 69 of The Data Protection Act 2018. The Data Protection Officer monitors internal compliance with data protection matters, provides advice and information on data protection obligations, acts as a contact point for data subjects and the Information Commissioner's Office. The Data Protection Officer is independent and has direct communication with the Board.

The Senior Information Governance Managers have overall operational responsibility for the Trust's information governance function, managing the work of the information governance team, ensuring information governance is proactive and effective in supporting best practice for ELFT staff and best care for ELFT's service users.

The Information Governance Managers (London and Bedfordshire & Luton) will, under the direction of the Senior Information Governance Manager – Systems, oversee the systems and procedures that support the implementation of this policy, co-ordinate any subject access requests where it is unclear where the requester's personal information is located, and provide support and advice where the request is sensitive or complex. The Information Governance Managers will liaise with the Trust's Data Protection Officer when required.

The Information Rights Coordinator will support the local Access to Records leads, manage a caseload of complex requests and track the performance of the Information Governance Team through the collation of performance statistics from Access to Records leads across the Trust.

Designated local Access to Records leads will have a system in place to respond to requests promptly, within agreed timescales, will identify any exemptions and third party information and will ensure the information is reviewed by an appropriate individual prior to its release.

Individuals responsible for reviewing and approving information for release in response to a subject access request will do so within in a timely manner that enables release of the information within statutory timeframes.

All individuals accessing personal information in response to a subject access request or for other purposes must understand and comply with the law, Confidentiality Code of Conduct and Trust Information Governance policies.

4.0 Rights of access to records containing the personal information of living individuals

Individuals have the right to be informed if the Trust holds personal data about them and in most circumstances to be given a copy of that data, irrespective of when it was compiled. The following sections set out the relevant legislation, who may apply for access, fees, time limits and an outline of the process Access to Records leads follow when dealing with subject access requests.

5.0 Who may apply for access

5.1 Access by an individual

The following individuals may apply for access:

- **Competent service users** - may apply for access to their own records subject to certain exemptions, or may authorise third parties such as lawyers, employers or insurance companies to do so on their behalf. It is not necessary to give a reason why.

- **Children and young people -** competent young people may apply for access to their own records. Legally there is no automatic presumption of capacity for individuals under the age of 16 so they must demonstrate they have sufficient understanding. Where in the view of the health professional a child is considered capable of making decisions about his/her medical treatment, his/her consent should be sought before a parent or other third party can be given access to the child's personal information. However, children aged 12 or over are generally expected to have the capacity to give or withhold consent to the release of information from their health records.

- **Staff, contractors, volunteers –**

  Individuals currently employed by the Trust should contact their local People & Culture Adviser if access to their HR file is required. Where an individual requires information that may be held by a line manager or other individuals, a written request must be submitted to the Access to Records team (elft.accesstorecords@nhs.net). Identification will be required unless an East London NHS Foundation Trust email address is used.

  Ex staff, contractors or volunteers should submit their requests directly to the Access to Records team. Identification will be required.

  All requests must be explicit in what is required, give details of who may hold the information, the time period required and the subject matter of the data required.

  Requests will be processed by asking the individuals who hold personal data relating to the requester to disclose that data directly to the Access to Records team. If this is not acceptable it may not be possible to respond to the request. Requesters should note that all staff contracts contain a confidentiality code of conduct and that any deliberate withholding of information may result in action being taken against that individual.

5.2 Access by someone acting for an individual

- **Parents -** may have access to their children's records if this is not contrary to a competent child's wishes. Any person may apply for parental responsibility but not all parents automatically have parental responsibility. For children born after 1st December 2003 both biological parents have parental responsibility if they are registered on a child's birth certificate. For children born before this date, a child's biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or sometime thereafter. If the parents have never been married only the mother has automatic parental responsibility but the father may acquire that status by order or agreement. Neither parent loses parental responsibility on divorce. Where more than one person has parental responsibility each may independently exercise rights of access.

Where a child lives with one or other parents there is no obligation to inform the parent the child lives with if the other parent seeks access to the records of the child, providing the parent seeking access can demonstrate parental responsibility as outlined above.

Where a child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility.

In some circumstances people other than parents acquire parental responsibility for example the appointment of a guardian or on the order of a court. A local authority acquires parental responsibility (shared with the parents) whilst a child is the subject of a care or supervision order.

The Trust is entitled to refuse access to a parent or individual with parental responsibility if knowledge of the information contained in the child's record could cause serious harm to the child or another individual.

- **Next of kin -** the term 'next of kin' does not have a formal legal status. A next of kin has no rights of access to medical records and cannot give or withhold consent to the sharing of information on a patient's behalf.
- **Solicitors -** information can be released to solicitors provided the patient has given signed and valid consent to the disclosure. If there is any doubt that the patient understands the nature and extent of the information being disclosed, the health professional should discuss this with the patient prior to disclosure.
- **Solicitors acting for another party -** consent from the patient should be obtained prior to disclosing any information. If the patient refuses, or the health professional does not consider it appropriate to disclose, the solicitor may apply to the Court for an Order requiring disclosure.
- **Individuals on behalf of adults who lack capacity -** an individual's mental capacity must be judged in relation to the particular decision being made. If the health professional believes the patient has the requisite capacity to give or withhold consent to the disclosure of information then their consent is necessary where a relative or third party requires access to their records.

  Where the patient does not have capacity, information may be shared with any individual authorised to make proxy decisions. The Mental Capacity Act contains powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults (see below). The Court of Protection can also appoint deputies for this purpose. This may entail giving access to relevant parts of a patient's medical records unless the health professional can demonstrate this would not be in the patient's best interests.

- **Power of Attorney –** there are two types of Power of Attorney:

  - An ordinary Power of Attorney (PoA) gives another person the power to act on an individual's behalf with regard to property or financial affairs. It does not include health matters and does not give a right of access to an individual's health record without the consent of that individual.

  - An Enduring Power of Attorney (EPA) does not extend to personal welfare and therefore does not give the right of access to health records of another individual.

- A Lasting Power of Attorney (LPA) replaced the Enduring Power of Attorney in October 2007 as part of the Mental Capacity Act 2005. It relates either to property and affairs or to personal welfare. It can only be used in the event of an individual's mental incapacity and must be registered to take effect. Health information of another individual can only be disclosed where there is a Personal Welfare Power of Attorney. The Trust must be assured before disclosing health information that the individual lacks mental capacity.

- **Independent Mental Health Advocate (IMHA) -** a statutory form of advocacy that provides safeguards for certain qualifying individuals. An IMHA is entitled under the Mental Capacity Act 2005 to ask for access to the individual's health records and to make copies. No part of the record should be withheld from the IMHA.

5.3 Access to an individual's records by other agencies

- **Police -** if the police do not have a Court Order or warrant they may request voluntary disclosure of a patient's health records under Schedule 2 Part 1Paragraph 2 of the Data Protection Act 2018. There is no obligation to disclose records to the police. They should usually only be disclosed where the patient has given consent or there is an overriding public interest.

Disclosure in the public interest is made to prevent a serious threat to public health, national security, the life of an individual or third party or to prevent or detect serious crime. Serious crime includes murder, manslaughter, rape, treason, serious fraud, state security and kidnapping or abuse of children or other vulnerable people. It does not include theft, minor fraud or damage to property. See also the section on other legislation and statutory requests.

- **Other NHS Trusts -** If a service user has transferred care then the records are transferred to the new provider on receipt of a written request to the access to records team. Consent is not required.

- In most other circumstances a patient should give consent for copies of medical records or a medical report to be sent to another Trust. This does not apply where the patient refuses consent and it is in the public interest to disclose the information, for example, when someone is at risk.

Where a request is received by another health or social care organisation or a third party such as a solicitors, requesting specific information about a patient this should be directed to the most appropriate clinician or health professional involved or most recently involved in the patients care to respond to.

The advice of the Information Governance Manager should be sought where clarification is required or where a request may be sensitive or contentious.

5.4 Access to the records of deceased people

The only statutory right of access to the records of deceased patients is under the Access to Health Records Act 1990. The Act provides a small cohort of people with a statutory right to apply for access to information contained within a deceased person's record. These individuals are defined under Section 3(1)(f) of the Act as 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the Executor or Administrator of a deceased person's estate.

A personal representative has an unqualified right of access to a deceased person's record and need give no reason for applying for access. Other individuals have a right of access only where they can establish a claim arising from a patient's death. Only information directly related to the claim should be disclosed.

Requests must be responded to within 21 calendar days.

In some circumstances individuals who do not have a statutory right of access under the Act may request access to a deceased person's record, such as helping a relative to understand the cause of death or the actions taken to ease the patient's suffering. Whilst longstanding legal advice is that the duty of confidentiality extends beyond death, requests should be considered on a case by case basis, be proportionate, in the public interest and not simply rejected. Consideration should include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following disclosure, any loss of privacy that might result and the impact on the deceased's reputation.

The advice of the Information Governance Manager should be sought where clarification is required or where a request may be sensitive or contentious.

6.0 Relevant legislation

6.1 Data Protection Act 2018

Section 45 of the Data Protection Act 2018 gives living individuals or their authorised representative the right to apply for access to their personal data. It applies equally to all relevant records and is not confined to health records.

An individual who makes a written request is entitled to be:

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons for its processing, and whether it will be shared with other individuals or agencies
- Given a copy of the information or to access it on Trust premises
- Where available, given details of the source of the data

Requests must be responded to within one calendar month.

The Trust does not normally make a charge for individuals or third parties (such as solicitors) who make a subject access request. Please see more details on the Fees section.

6.2 Access to Health Records Act 1990

If an applicant requests access to the records of a deceased patient, the only right of access is under the Access to Health Records Act 1990. There is an ethical obligation to respect a patient's confidentiality beyond death. This is also set out in Section 41 of the Freedom of Information Act 2000.

The section on the 'Rights of access to the records of deceased people' explains this in detail.

6.3 Access to Medical Reports Act 1988

This Act governs access to medical reports written by a medical practitioner who is / has been responsible for the clinical care of a patient for insurance or employment purposes. A third party cannot ask for a medical report for employment or insurance reasons without the individual's knowledge and consent.

The individual can apply for access to the report at any time before it is supplied to the employer / insurer, subject to certain exemptions including where it would cause serious physical or mental harm to the individual or a third party or identify a third party who has not consented to the release of that information.

It should not be supplied to the employer / insurer until the individual has been given access unless 21 days have passed since the individual has communicated about making arrangements to see the report. Once access has been given it should not be supplied to the employer / insurer until the individual has consented. Individuals have the right to request in writing amendments to the report if any part is incorrect or the right to have attached a note of their views if the medical practitioner declines to amend the report. Individuals also have the right to refuse to consent to release of the report.

The Trust makes a charge for requests made under this Act. These charges are laid out in the Fees section.

6.4 Other legislation and statutory requests

- **Court Orders –**there is a legal duty to disclose information in response to an order of the Courts. The advice of the Information Governance Manager should be sought prior to disclosing information. These are usually urgent, are unequivocal and failure to respond can result in staff being subpoenaed to appear in Court. It is not necessary in most circumstances to seek the consent of the individual whose information is being requested. The Information Governance Manager will advise on a case by case basis.

- **Road Traffic Act 1988 –** when asked, there is a legal duty to provide the police with the name and address of a driver who is allegedly guilty of an offence under this Act. Clinical information should never be disclosed. There is no duty to advise the police when an individual is likely to attend an appointment at the Trust. It is not necessary to seek the consent of the individual whose information is being requested.

- **Prevention of Terrorism Act 1989 and Terrorism Act 2000 –** there is a legal duty to inform the police if information is known about terrorist activity, including personal information. It is not necessary to seek the consent of the individual and it may endanger safety if the consent of the individual is sought.

- **Police and Criminal Evidence Act –** the Trust may pass on information to the police if it is believed someone is at serious risk of harm or death. Serious arrestable offences include murder, rape, kidnapping and causing death by dangerous driving. They do not include minor offences such as theft. The Trust should consider whether it is appropriate to seek the consent of the individual prior to disclosure.

- **Children Act 1989, sections 17 and 47 –** the police or local authority may make enquiries when deciding whether to take action to safeguard a child's welfare. Consent does not have to be gained from the child or parents but it is good practice to do so if appropriate.

- **Crime and Disorder Act 1998, section 115 –** the Act provides for anti-social behaviour orders to be applied by the police or local authority against individuals aged ten or over. Section 115 of the Act permits the disclosure of personal information that may otherwise be prohibited. There is no duty to disclose. This means information given in confidence should not be disclosed unless there is a clear public interest in doing so as the conditions of the Data Protection Act 2018 and the common law duty of confidence apply.

7.0 Duty of confidence

All individuals within the Trust have a duty of confidence. This is included in employment and other contracts. This means any personal information given or received in confidence for one purpose should not be used for a different purpose without the consent of that individual or their representative unless there is a legal duty to do so.

8.0 General procedure for dealing with subject access requests

8.1 Receipt and appraisal of new requests

All requests for access to personal information should be forwarded to the local Access to Records Lead, who will ensure appropriate consent from the individual who is the subject of the request, has been received.

Once appropriate consent has been received, the Access to Records Lead will co-ordinate the process and ensure the disclosure is made within the relevant timescale. This applies to requests for access to the personal information of both staff and service users.

A list of Access to Records Leads is available from the Information Rights Team.

The process below should be followed by Access to Records Leads. All individuals have a duty to pass any requests promptly to the relevant lead for action.

Access to Records leads should seek the advice an Information Governance Manager where clarification is required or a request may be sensitive or contentious.

8.2 Dealing with general requests and queries

Where general requests for information are received, or it is unclear which Access to Records lead should be contacted, the Information Rights Manager's team will undertake the following actions:

- **Requests from staff / contractors / volunteers not currently working in the Trust- -** ensure relevant identification is received, acknowledge receipt to requestor and subsequently liaise with HR, who will provide the information requested to an Information Governance Manager. The Information Governance Manager will then co-ordinate the request and provide all disclosable requested information. This is not limited to HR records and dependent on the request, may include the co-ordination of emails, minutes of meetings etc.

- **Requests from patients where it is unclear where care was received –** perform a search on RiO or ask other electronic clinical systems owners to check to see if the patient can be identified, acknowledge the request with the requester (advising where the care was received and who to contact) and pass to the relevant Access to Records lead. Where care has been received in more than one Directorate and the requester wishes to receive all their personal information, the Access to Records lead where care was last received will co-ordinate the process

- **General requests from the police / other agencies -** perform a search on RiO or ask other electronic clinical systems owners to check to see if the patient can be identified then advise the police / other agency who should be contacted for access to the records if there is a just reason for disclosure.

9.0 Guidance for Access to Records leads

9.1 Reasons for requiring access

There is no obligation for an individual or third party acting on behalf of an individual to state why access to their personal information is required.

It is helpful to encourage individuals to state what information is required, especially where it relates only to a particular episode of care or period of employment. The form at Appendices 1 - 2 can be used for this purpose.

9.2 Intended litigation

Solicitors or anyone acting in a legal capacity must confirm if litigation is intended against the Trust. The Legal Affairs Department (elft.legalservices@nhs.net) must always be notified by the Access to Records lead where litigation is intended. This must be within five days of receipt of the request and before any disclosure takes place.

9.3 Confirming identity

The Trust must satisfy itself as to the identity of the person making the request to ensure information is released only to the data subject or to a third party with the data subject's consent. The clock does not start until identification has been confirmed.

All requests can be in writing or verbal and must be accompanied by proof of identity. Applications should be accompanied by photocopies of two different official documents which between them provide sufficient information to prove the name, date of birth, current address and signature of the individual whose personal information is sought. For example, driving license, medical card, birth certificate, passport, bank statement (with financial information redacted) utility bill.

The form on the information governance forms page on the intranet can be used for this purpose.

Personal representatives of deceased people are required to provide evidence of their right to act in this capacity.

The Trust will refuse to comply with a request until identification has been confirmed. This may, however, be waived in extenuating circumstances where there is absolutely no doubt regarding the identity of the applicant. Service users currently admitted to a ward do not need to provide identity whilst receiving inpatient care. Discretion may also be used where a service user receiving community care makes a face to face request to the individual currently providing their ELFT care. The individual proving care must be assured the service user genuinely wants access to their records and is not being unduly influenced by their family, carers or friends.

The police, Courts and other agencies acting in an official capacity are not required to provide proof of identity.

9.4 Consent

Where a third party applies for access to the records of an individual, the individual must give explicit (written) consent.

There is no legal time limit after which consent to disclose becomes invalid. However, if there has been a significant interval between the time written consent was provided and the time the request was made, it is good practice to confirm the data subject is still willing to agree to the disclosure. This is particularly important if the request is made via a solicitor or insurance company, where it is believed the individual may now have a different view, or where the capacity to consent may have changed.

Applications from Solicitors will be accepted without identification documentation providing the request is received on headed notepaper and is supported by the signed consent of the data subject.

Applications from other Third Parties will be accepted providing the identity of the data subject is confirmed, as above, signed consent is given by the data subject and the Third Party can evidence a valid name, address and relationship to the data subject.

Consent to disclose to the police and other agencies is not always necessary. The advice of the Information Governance Manager supervising the request should be sought prior to disclosure.

9.5 Processing and responding to requests

The flowchart in Section 10 should be followed by Access to Records leads when processing requests.

The relevant requests templates on the information governance forms page on the intranet can be used for this purpose.

The relevant letter templates on the intranet should be used by Access to Records leads when responding to requests for disclosure of personal information.

The following principles apply:

- All requests can be verbal or in writing
- Appropriate consent should be obtained prior to releasing the information. The clock stops until valid consent is received
- Local Access to Records leads should co-ordinate the subject access process
- Services should clearly display information advising service users how to obtain copies of their records
- In exceptional circumstances information may be withheld from a service user. This is usually where it would identify a third party who has not consented to the release of their information or where release might affect the rights and freedoms of the service user or other individuals. Please ensure that a copy of what was withheld (redacted) is kept in the relevant network drive.
- The Responsible Clinician or lead care co-ordinator must make the decision to refuse access to records. This should be clearly documented in the records. The service user should be notified in writing of the decision. Care should be taken that third party information is not inadvertently released in writing to the service user

9.6 Fees

The subject cannot be charged for copies of records unless the request is 'manifestly unfounded, excessive or repetitive'. You could then charge a reasonable fee. There is currently no agreed definition of what constitutes a manifestly unfounded or excessive request, or what a reasonable fee is. This type of request will be rare. If in doubt, please contact the Information Governance Manager. Third parties requesting access on behalf of service users/patients cannot be charged either.

9.7 Response targets

The following response times apply:

- One calendar month under the Data Protection Act 2018 for the records of living people and 21 calendar days under the Access to Health Records Act 1990 for the records of deceased people.

- All requests should be acknowledged within five working days of receipt.

Note that the clock stops until any clarification/information sought is received.

9.8 Minimum periods between requests for access

Where a request has previously been complied with there is no obligation to give access again until a reasonable period has elapsed. Reasonableness depends on the nature of the information, whether it has been updated, and to some extent, the reason for the request.

Contact the Information Governance Manager for further advice.

9.9 Approval from an appropriate health professional

All disclosures from patients' health records must be approved by:

- The patient's Responsible Clinician or the lead Health Care Professional
- A professional nominated by the locality clinical director where the above person has left the Trust

The Responsible Clinician Approval form on the intranet should be completed by the health professional and forwarded to the Access to Records lead before any information is disclosed to the patient or representative.

9.10 What must be disclosed

All records (subject to the caveats outlined in 'Grounds for refusing disclosure') relating to the physical or mental health of an individual should potentially be disclosed in response to a request for access to health records. This includes all paper and electronic records including X-rays, ECGs, complaints, incident investigation files etc.

Staff, ex staff, volunteers etc are entitled to be given a copy of any personal information about them. This is not limited to information contained in their HR record and may include emails, reports, minutes of meetings etc.

Applicants are entitled to be given a copy of the records or alternatively to view them on Trust premises if preferred. Copies of records disclosed must be stapled together in relevant sections and where appropriate include section tabs and a front cover.

9.11 Grounds for refusing disclosure

Information should not be disclosed if:

- Disclosure would be likely to cause harm, damage or distress to the physical or mental health of the data subject or another individual
- Disclosure would identify another individual who has not given permission for

the information to be released. This does not apply to health professionals caring for the patient or individuals acting in a work context

- A third party agency has expressly not consented to disclosure of the information
- There is a duty of confidence to the individual. This includes where the information was given in the expectation it would not be disclosed to the person making the request or an individual has expressly stated it should not be disclosed to a particular individual. It also applies to the records of a young person where the young person is considered competent to make their own decisions and to information relating to an incapacitated person
- The information is subject to legal professional privilege (such as an independent report written for the purposes of litigation)
- The information is restricted by order of the Courts
- The request is vexatious. Seek the advice of the Information Governance Manager prior to responding to the request
- The information is not kept in a structured filing system i.e. there is no logical way of retrieving it. Seek the advice of the Information Governance Manager prior to responding to the request
- Where applicants have a claim arising out of a patient’s death, access can only be given to the part of the record that is relevant to the claim
- If the Responsible Clinician / HCP states they would prefer to counsel the applicant prior to releasing the information. In this case the Access to Health Records lead should write to the applicant to offer an appointment

It is not necessary to advise why information is withheld. However, where information is partially redacted in response to the above points there is an obligation to disclose the remainder of the records.

9.12 Explanation of medical terms

Any terminology that might be unintelligible to the requester should be explained. As levels of understanding vary, applicants should always be advised to contact the Trust if anything is unclear or an explanation is required.

9.13 Correcting inaccurate information

Individuals have the right to seek correction of information they believe is inaccurate. Where the Trust does not accept the individual’s opinion the opinion must still be recorded.

Requests must be made in writing, clearly stating what needs amending and what it should be amended to. Service users and other individuals seeking correction are not permitted to alter their own records as the Trust has a responsibility to maintain them to professional standards. In the case of electronic records, service users and unauthorised individuals are not permitted to access electronic systems to make amendments as they do not have an authorised Trust log in.

The right of rectification only applies to factual information and not opinions made by professionals. Factual inaccuracies (such as the wrong date of birth) may be corrected. Note that the information originally supplied should not be erased as it must be available as part of the original record.

Clinical opinion, whether accurate or not, and observations may not be amended or destroyed as they form an important part of the service user’s care. Information supplied by third parties should also not be amended. In these instances the service user's opinion should be noted on the record.

In the case of health records, retention of relevant information is essential for understanding decisions that were made at the time and to audit the quality of care.

Individuals have the right to be supplied with a copy of the correction or appended note.

Individuals also have the right to request erasure of information held about them, also known as the right to be forgotten. The right to erasure does not normally apply to health records, however requests should be reviewed and processed in line with The Data Protection Act 2018.

If an individual asks for rectification or the deletion or erasure of information the Trust holds about them, the request should be sent to the relevant manager, clinician or health care professional who should contact the Information Governance Manager to discuss the request which will be reviewed on a case by case basis so the Trust meets its obligations under section 46 and 47 of the Data Protection Act 2018. Discussion with the individual and the subsequent decision rests with the clinician and not with the Information Governance Manager.

Third parties must be notified so that they can also update/correct their records. Individuals have the right to challenge the Trust's decision through its complaints process, and ultimately via the Office of the Information Commissioner.

9.14 Requests for CCTV Footage

If a subject access request requires the review and/or disclosure of CCTV footage, the service (ward, department, etc.) from which CCTV footage is requested will be responsible for securing the footage in accordance with the Trust's CCTV Policy. The relevant service will also conduct any necessary redactions to protect the privacy of individuals not involved in the incident under investigation before disclosing the footage. The service may obtain guidance from an Information Governance Manager.

10. Monitoring

Access to Records Leads will provide statistics on volume and compliance status of subject access requests to the Senior Information Governance Manager - Systems, who will then report to the Information Governance Steering Group.

11. References

The following can be found at *www.**legislation**.gov.uk*

Access to Health Records Act 1990
Data Protection Act 2018
Access to Medical Records Act 1988
Road Traffic Act 1988
Prevention of Terrorism Act 1989 and 2000
Police & Criminal Evidence Act
Children's Acts 1989
Crime & Disorder Act 1998 section 115

12. Associated Documents

Health Records Policy
Non Health Records Policy
Information Governance Strategy
Information Governance and IMT Security Policy
Closed Circuit Television Policy

To be sent with disclosures to individuals

In accordance with Section 45 of The Data Protection Act 2018 we are providing you with this general information about your personal data.

We process and share your personal data in line with the Health & Social Care Act 2015, Data Protection Act 2018.

We process your personal data to help provide you with the best possible healthcare. We share it for health and social care purposes. Not sharing information may lead to a clinical risk, safeguarding concerns or concerns about your care and may have an impact of the care we or our partners can provide. Where it supports your care we may also share your information with education and voluntary and private sector agencies. We also receive information about you from other health, social care and other agencies, and from individuals such as your carers or family. In most circumstances we do not share information about you with other individuals unless you have given us your consent.

We process basic information about you (name, address and contact details). We also process special category personal data. This is your health information. If we need it to care for you we may process other special category personal data such as your religious beliefs or sexual preferences.

We keep your personal information according to the NHS Records Management Code of Practice https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

If you think the information we hold about you is incorrect please state this in writing to elft.information.governance@nhs.net . We are able to change incorrect factual information. We are not able to change clinical opinions. If you think these are wrong, set out ahy you think this and we will add it to your clinical record.

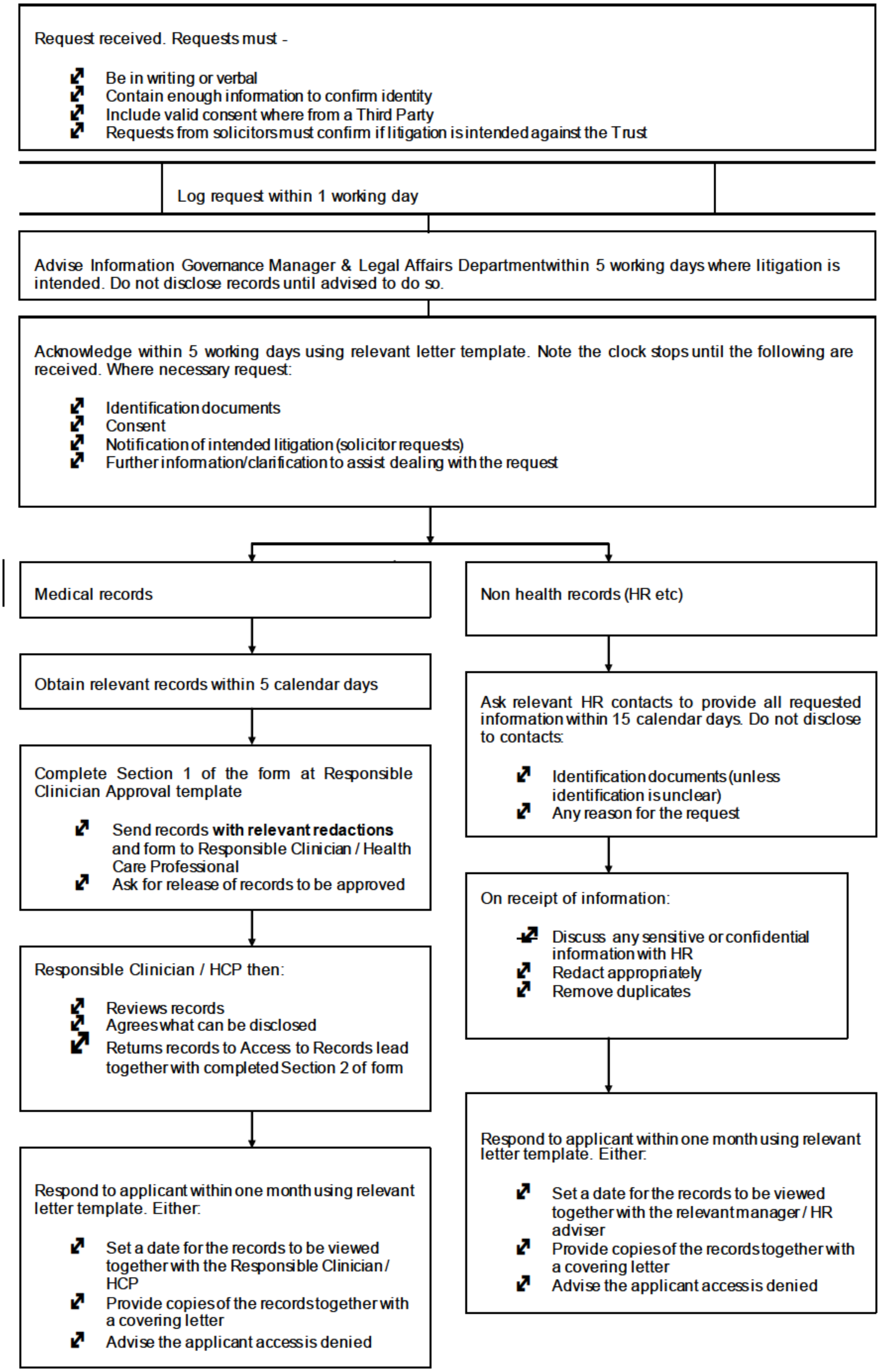
We do not use automated decision making to make any decisions about you.

We do not send your personal data to another country or to any international organisations.

You have the right to complain about the way we process your personal data. You can contact your clinical team, speak to our PALS team at elft.palsandcomplaints@nhs.net, or contact our Data Protection Officer at elft.dpo@nhs.net .

If we are unable to resolve your concern you have the right to complain to the Information Commissioner. Call their helpline on 0303 123 1113 (local rate – calls to this number cost the same as calls to 01 or 02 numbers). Or see the ICO website https://ico.org.uk/

13. Procedure flowchart for Access to Records leads



Request received. Requests must -

- Be in writing or verbal
- Contain enough information to confirm identity
- Include valid consent where from a Third Party
- Requests from solicitors must confirm if litigation is intended against the Trust

Log request within 1 working day

Advise Information Governance Manager & Legal Affairs Department within 5 working days where litigation is intended. Do not disclose records until advised to do so.

Acknowledge within 5 working days using relevant letter template. Note the clock stops until the following are received. Where necessary request:

- Identification documents
- Consent
- Notification of intended litigation (solicitor requests)
- Further information/clarification to assist dealing with the request

Medical records

Obtain relevant records within 5 calendar days

Complete Section 1 of the form at Responsible Clinician Approval template

- Send records **with relevant redactions** and form to Responsible Clinician / Health Care Professional
- Ask for release of records to be approved

Responsible Clinician / HCP then:

- Reviews records
- Agrees what can be disclosed
- Returns records to Access to Records lead together with completed Section 2 of form

Respond to applicant within one month using relevant letter template. Either:

- Set a date for the records to be viewed together with the Responsible Clinician / HCP
- Provide copies of the records together with a covering letter
- Advise the applicant access is denied

Non health records (HR etc)

Ask relevant HR contacts to provide all requested information within 15 calendar days. Do not disclose to contacts:

- Identification documents (unless identification is unclear)
- Any reason for the request

On receipt of information:

- Discuss any sensitive or confidential information with HR
- Redact appropriately
- Remove duplicates

Respond to applicant within one month using relevant letter template. Either:

- Set a date for the records to be viewed together with the relevant manager / HR adviser
- Provide copies of the records together with a covering letter
- Advise the applicant access is denied

NHS
East London
NHS Foundation Trust

Data Protection and Confidentiality Policy

Version number :	1.3
Consultation Groups	Quality Committee
Approved by (Sponsor Group)	Information Governance Steering Group
Date approved	11th February 2025
Ratified by:	Quality Committee
Date ratified:	26th March 2025
Name of originator/author:	Data Protection Officer
Executive Director lead :	Chief Quality Officer
Implementation Date :	April 2025
Last Review Date	March 2025
Next Review date:	March 2028

Services	Applicable
Trust wide	X
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0	03.12.18	Information Rights Manager	Final	New policy providing guidance on data protection and confidentiality.
1.1	18.07.2019	DPO	Final	Updated to include committee structure, Information Asset Owner responsibilities, DPO requirement
1.2	03/2022	DPO	Final	Updated to include changes to SIRO, Executive oversight & operational responsibilities
1.3	01/2025	DPO	Final	Routine review. Fax as a method of communication removed. GDPR conditions for sharing information added. Job roles updated. Information governance content extracted from Information Governance & IMT Policy to become a standalone policy

Contents

Executive Summary

This policy provides a guide to the key elements of the legal framework governing information handling, outlines the responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling.

1.0 Introduction and purpose

1.1 Introduction

The Data Protection Act (2018) and the UK General Data Protection Regulation set the legal framework by which the Trust can process personal information. They apply to information that
might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) Article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A). It applies to all areas of the Trust and all staff who handle information.

Data protection and confidentiality is a component of information governance and as such this policy and associated procedures form part of the Trust's overall Information Governance Framework.

1.2 Purpose

The objectives of this policy are:

- To outline the ways in which patient and staff data is handled effectively and securely
- To promote best practice and innovative use of personal information, especially to inform care and research
- To ensure responsibilities and obligations are understood

2.0 Duties and responsibilities

2.1 Management responsibilities

The **Chief Executive** is the Trust's **Accountable Officer** and responsible for overall leadership and management of the Trust with the ultimate responsibility for ensuring compliance with the Data Protection Act (2018), the UK General Data Protection Regulation, Human Rights Act (1998) and the Common law Duty of Confidentiality. The Chief Executive delegates aspects of her responsibility to relevant executive directors according to their organisation portfolios.

The **Chief Quality Officer** is the **Senior Information Risk Officer (SIRO).**

The Associate Director of Information Governance is the **Data Protection Officer** and Responsible for managing data protection issues throughout the Trust. A Data protection Officer is a legal requirement under Article 37 of the General Data Protection Regulation. The Data Protection Officer monitors internal compliance with data protection matters, provides advice and information on data protection obligations, acts as a contact point for data subjects and the Information Commissioner's Office. The Data Protection Officer is independent and has direct communication with the Board.

The Chief Quality Officer has executive responsibility for information governance including chairing the **Information Governance Steering Group,** where data protection issues are discussed and escalated to relevant groups and committees when necessary.

Day to day responsibility for data protection and confidentiality management is the responsibility of **Senior Information Governance Managers** and the **Information Governance Managers.**

The **Chief Medical Officer** is the **Caldicott Guardian** with specific responsibility for the confidentiality agenda and the collection, use and sharing of patient information.

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

Service Directors / Associate Directors are Information Asset Owners, supported by **Team Managers** who are Information Asset Administrators.

All **Managers** are responsible for the local implementation of this policy in their areas of responsibility.

2.2 Individual responsibilities

Everyone working for the NHS has a legal duty to keep information about service users and other individuals such as staff or volunteers confidential. Staff are required to adhere to confidentiality agreements, e.g., common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

The terms and conditions within Trust employment contracts include specific conditions relating to confidentiality which must be adhered to.

All members of staff are responsible for ensuring they keep up to date with Information Governance/Data Security training in accordance with the Trust Statutory and Mandatory training needs analysis.

The need for data security training also applies to agency staff, contractors and volunteers working at the Trust who may have access to personal information. Most agencies working with the NHS provide their staff with this training. Where this is not the case, local arrangements should be made to ensure the employee is adequately trained before working at the Trust.

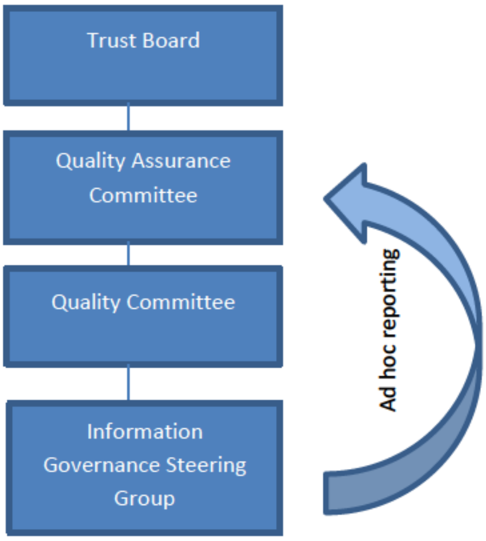
All users must sign a confidentiality agreement, either as part of their contract or as a separate confidentiality agreement. Furthermore, individuals with privileged access to systems are required to sign an enhanced agreement to ensure they take their responsibilities seriously.

3.0 Reporting structures

The Information Governance Steering Group oversees the information governance agenda and is responsible for holding the information governance function to account.

The Information Governance Steering Group is a subcommittee of Quality Committee. Quality Committee receives quarterly update reports on information governance matters plus any exception reporting. It ratifies policies approved at Information Governance Steering Group.

The Quality Assurance Committee is a Board subcommittee. Quality Committee reports to the Quality Assurance Committee. The quarterly reports tabled at Quality Committee are summarised at Quality Assurance Committee. Ad hoc information governance reports including the annual SIRO report are regularly tabled at Quality Assurance Committee.


Trust Board
Quality Assurance Committee
Quality Committee
Information Governance Steering Group
Ad hoc reporting

4.0 Principles

To appropriately balance openness and confidentiality, the Trust places importance on the confidentiality and security of data to safeguard both personal information about patients and staff and commercially sensitive information. It 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.

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 data protection policy:

- **Openness:**
  - Non-confidential information about the Trust and its services is available to the public through a variety of media, in line with the Trust's code of openness
  - Policies are established and maintained to ensure compliance with the Freedom of Information Act, data protection and other associated legislation
  - Service users must in most circumstances have ready access to information relating to their own health care, their options for treatment and their rights as patients

- **Legal compliance:**
  - All identifiable personal information relating to patients is confidential unless there is a legal reason to override confidentiality
  - All identifiable personal information relating to staff is confidential except where national policy on accountability and openness requires otherwise

- **Information security**
  - Policies are established and maintained to ensure information assets are secure. This is set out in the Trust's IMT Security policy

- **Quality assurance**
  - Policies are established and maintained to ensure information quality assurance and records management. This is set out in the Data Quality policy

- Pseudonymisation will be used where de-identified data is required (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). Advice should be sought from the Informatics team where pseudonymisation is necessary.

5.0 Data Protection Act 2018 and UK GDPR

The Data Protection Act (2018) (DPA) and the UK General Data Protection Regulation (GDPR)
set out the legal requirements and duties placed on data controllers (i.e. the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information
rights' held by data subjects (individuals we hold information about).

As a Data Controller, the Trust is required to register annually with the Information Commissioner. The Trust's unique registration number is **Z5601596.**

The Data Protection Act (2018) defines six Data Protection Principles which all processors of personal information must abide by:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

The Data Protection Act (2018) does not apply to deceased persons. The Access to Health Records Act 1990 governs the access to health records of deceased patients. The NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought from the Information Governance Team: elft.information.governance@nhs.net

Under GDPR each controller of personal information must decide under what basis it is processing personal information. If there is no relevant basis, then the processing is likely to be
unlawful.

- Under Article 6, the Trust's basis for processing personal information is usually:
- Article 6(1)(e) the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- As the Trust processes special category information – which includes health data then it must have a second basis (under Article 9), which is usually:
- Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

The UK 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.

6.0 NHS Caldicott Report

The 1997 Caldicott Report (updated in 2013 and 2016) focusses on the protection and processing of patient identifiable information within the NHS. The reports provide the NHS with eight principles:

- Justify the purpose for collecting or holding patient-identifiable information
- Use confidential patient-identifiable information only when necessary
- Use the minimum necessary information
- Access to confidential information should be on a strict need to know basis
- Everyone with access to confidential information should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Inform patients about how their confidential information is used

The Caldicott Guardian advises the Trust Board on matters of patient confidentiality and promotes the safe and secure handling of patient data. The Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures, where there are ethical considerations.

7.0 Data processing

Data processing is the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintain confidence between the Trust and its patients, staff and others. The DPA requires that processing of any personal information must be both fair and lawful. Processing must meet fair processing criteria and satisfy one or more ‘conditions for processing’ set out in the DPA. 5.3.3. We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- help people to understand their rights

To meet this requirement the Trust publishes a fair processing notice to inform individuals about the way we handle and use their personal data. This is published on the Trust’s public website.

Routine data processing for the purposes of patient care will normally satisfy one of the processing conditions in the DPA. When sharing takes place for non-care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information.

8.0 Access to IT systems

IT systems holding personal data must have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

The Information Governance & IMT Security Policy provides detailed guidance on the security of
Trust IT systems including minimum standards of access controls.

Individuals should not attempt to access or use electronic record systems they have not been trained to use or are not authorised to access. Existing system users should not allow others to access systems using their login credentials. Action may be taken against individuals who share passwords and Smartcards.

9.0 Accessing records

The Trust holds individual service user records in a variety of formats. In addition, it holds personal records for present and former members of staff and others it does business with. While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is not allowed and may be unlawful. Appropriate action will be taken against any individual contravening this standard.

Digital systems may allow a user to access any individual record held in that system. Users should only access records where they have authorisation to access them for specific purposes
or in the case of health records where they have a 'legitimate relationship' with the service user.

Staff have no right to access personal information held in records about their relatives, colleagues or friends.

Staff should not access their own data held in any Trust systems without specific authorisation. Instead they should make a subject access request.

Procedures for obtaining access to or copies of health records about individuals that are held by the Trust are explained in the Access to Health Records Policy.

The Trust carries out audits of access to personal data and any individual who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' records / data may face action.

10.0 Communicating personal information

To provide effective care there is a need to transfer information between organisations and individuals. To comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

Any electronic data containing identifiable information transferred outside the Trust for processing must be securely encrypted during transit. Any transfer outside the European Economic Area must only be carried out if appropriate security controls are in place.

A guide on the transfer or communication of personal data by post, hand, e-mail and other methods of electronic communication is available on the intranet. Fax should not be used. Written communications containing personal information must be in a sealed envelope and addressed by name to a designated person. Judgement should be used on the appropriateness of using tracked / recorded delivery. Post should be marked "Personal and Confidential – to be opened by the recipient only".

11.0 Disclosure and sharing of personal information for care purposes.

To provide safe and effective care, personal information about service users will be shared not only with the clinical team providing care, but also the direct care team which may include
pharmacy staff, social care staff, specialist care teams and administrative staff supporting the care process.

In accordance with the DPA 2018, GDPR and Caldicott principles information shared for care purposes should be relevant, necessary and proportionate. In applying this principle, care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

Caldicott Principle 7 (Duty to share) emphasizes the need to share information in certain circumstances where the need to share information clearly outweighs the normal duty of confidentiality owed, for example, when there is a threat to the safety of others and the sharing of personal information about individuals (e.g. vulnerable adults or children) with the police or other agencies may prevent a threat materialising.

GDPR Article 9(2)(h) permits the sharing of information without consent for the purposes of preventative or occupational medicine, or the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment

Disclosing information to relatives and carers

Staff will deal with numerous inquiries from relatives and friends of patients seeking information about progress and treatment. Many inquiries will be made over the telephone by people who are not registered as the patient's next of kin or carer and in these circumstances, it is sometimes difficult to decide if any information should be passed on. While in most circumstances a patient will not object to updates about their condition being given in response to an inquiry, circumstances do arise when this will not be appropriate. It is therefore good practice to establish and record if the patient wishes to place any restrictions on the information provided about them to others. This will make it easier to respond appropriately to any telephone inquiries received. Where restrictions are placed on information to be provided about patients it is important all staff likely to handle inquiries are made aware of the details to avoid a breach of confidentiality.

On receipt of an inquiry from a person not known to staff, where practical, the consent of the patient to disclose information should be sought. Where this is not possible a disclosure decision has to be made based on the information provided by the caller justifying their 'need to know'. Sensitive and detailed information should normally only be disclosed or discussed with nominated or recognised next of kin, close relatives or carers.

If suspicious about the motives of a person making an inquiry about a patient do not pass on any details but take a contact number and discuss with a senior colleague and seek advice before making contact again.

12.0 Sharing personal information for non-direct care purposes

Non-care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using anonymized or de-identified data. This removes the need to consider consent issues.

In certain circumstances the law requires that confidential information should be disclosed without consent. Examples of this include a direction within a court order to disclose confidential information or the requirement to notify Public Health officials when a patient is suspected of suffering from a notifiable disease.

Where a legal obligation to disclose does not exist there are some limited circumstances where the sharing of personal information without consent may be justified in the 'Public Interest'. Disclosures made without consent to support the detection, investigation and punishment of serious crime and to prevent abuse or serious harm to others are examples of such circumstances. Such disclosures are considered on a case by case basis and can be complex. The public good that would be met by sharing the information has to be weighed against the obligation of confidentiality owed to an individual and the public good in maintaining trust in a confidential service.

Disclosing information to the police

Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 provides a lawful basis for the Trust to disclose personal data about a person in the absence of their consent where this will support certain aspects of law enforcement and in particular:

- the detection, punishment and prevention of crime
- the identification, apprehension and prosecution of offenders

Unless there is a high harm threshold for the request (alleged homicide, threat to national security, serious sexual abuse) the police should provide the consent of the data subject prior to the Trust disclosing any information. Furthermore, all requests should be in writing. Each police force will have a specially designed template. Many inquiries made by the police will be handled first by the Information Governance Team or locality access to records leads. Occasionally inquiries will be made direct to wards and departments. The Information Governance team can provide advice if required.

Occasionally urgent requests will be made asking for specific information to be provided in a short period of time. Often this is due to strict timelines imposed on the police to make decisions to charge suspects or to support urgent lines of investigation. In these circumstances decisions may have to be made quickly but staff should not be pressured into disclosing information when they feel it is not in the patient's best interest. Note that in most circumstances the police should provide consent.

Whilst the law permits disclosure in the circumstances outlined above it does not compel the Trust to comply with such information requests. Each case should be considered on the individual merits of the request. Where consent to disclose information to the police is not provided or refused the Trust has to consider the duty of confidentiality owed to the data subject and the public interest in maintaining a confidential service and balance this with the wider public interest in making the requested disclosure to support law and order purposes. Striking the appropriate balance in some situations can be challenging and in these scenarios, where possible, staff should seek specialist advice from the Information Governance Team.

In addition to the police, other agencies such as the Home office, HMRC and NHS Counter Fraud Services may request information about patients using exemptions.

Sharing information for safeguarding purposes

Caldicott Principle 7 makes clear that in certain situations the duty to share information is as important as considerations of confidentiality. This is particularly the case in matters of safeguarding where in the past public authorities have failed individuals by not sharing information they have held which if passed on may have prevented someone harming them.

Where an individual is thought to be at risk, relevant information should be shared between agencies involved with the individual if the provision of that information might reduce or eliminate the identified risk. If it is possible to obtain consent from the subject to share their data this should be done, but the absence of or a refusal to provide consent should not deter staff from sharing information where it is felt to be appropriate and justified to support a safeguarding purpose.

Access to information for audit, service improvement and research purposes

Clinical audit – recognised as a necessary tool to check the care provided by the Trust meets acceptable standards and is safe and effective. Access to patient personal information (e.g. detailed medical records) without consent for the purpose of clinical audit is normally permissible. The audit should be internal to the Trust and not part of a multi-site/organisation audit and the audit would normally be registered with the Trust clinical audit service. Where these criteria are not met and access to patient information is requested advice should be sought before sharing information or allowing access to patient records.

Service improvement – dependent on the circumstances access to patient personal information without consent for the purpose of conducting a Service Improvement project may also be permissible. The term 'service improvement' is widely used to cover a range of improvement activities and caution should be exercised to ensure the boundaries between service improvement and research activities are not blurred.

Research – the Trust undertakes medical research and clinical trials. Most research activity requires formal ethical approval and patient consent is normally required before access to any patient personal information is provided or made. The need to obtain patient consent can be waived in some circumstances following formal application to the NHS Research Authority (NHSRA). Where access to medical records is required, the researcher must provide the reason for access, steps taken in order to maintain confidentiality and names and status of those needing access to notes. Those users must sign a declaration of confidentiality. Data subjects must be de-identified and signed consent must be obtained.

The flowchart at Appendix A sets out guidance on sharing information.

13.0 Consent

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

Obtaining consent

Consent is not normally required for direct care purposes. GDPR Article 9(2)(h) sets this out. 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.

Consent must be sought to share information with relatives, carers, friends etc

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 for non-direct care purposes is informed, and to set out rights for individuals, the Trust has a Your Records and You leaflet that explains:

The rights of individuals under the Data Protection Act 2018 and GDPR, particularly in relation to sensitive information.

- Procedures in place to enable clients/patients to access their records.
- 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.
- Circumstances under which information may be shared without consent and the procedures which will be followed.
- Complaints procedures to follow in the event that the individual concerned believes information about them has been inappropriately disclosed.
- How the information is recorded, stored and the length of time it will be retained

Recording consent

Consent for non-direct care purposes or for sharing information with family, friends etc 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.

Checking for consent

An individual's record must always be checked before personal information is disclosed for non-direct care purposes 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.

14.0 Disposal of personal information

It is a principle of the DPA that data should 'not be kept for longer than necessary'.
To assist staff in meeting this requirement the Trust adopts the retention schedule contained in the NHS Records Management Code of Practice.

All printouts, reports and printed copies of records containing personal data should be kept secure at all times. This particularly applies to handover reports and documents used by staff working in ward areas.

Any documents containing personal data should be disposed of securely and not discarded in domestic waste and recycling bins. The Trust operates a confidential waste disposal service and provides regular collections of confidential waste from all Trust areas.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops and any other devices with information storage capabilities) should be carried out through the Digital department to ensure all data is effectively removed before disposal.

The disposal of medical devices and equipment should follow the guidance on Decommissioning and Disposal provided in the Medical Devices Policy.

15.0 Breach of policy and procedure

Any breach of data protection and confidentiality can have severe implications for the Trust, service users and staff and can impact on the reputation of the NHS as a whole.

Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 may constitute a serious disciplinary offence or gross misconduct under the
Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

The Information Commissioner's Office (ICO) regulates data protection and is charged with upholding individuals' information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of financial penalties.

Staff must report incidents relating to data protection, data security and confidentiality and should follow the incident reporting procedures contained in the Trust Incident Reporting Policy.

Occasionally it may be necessary to access information on an individual's network account. The
rationale and process are set out in the IMT Security policy.

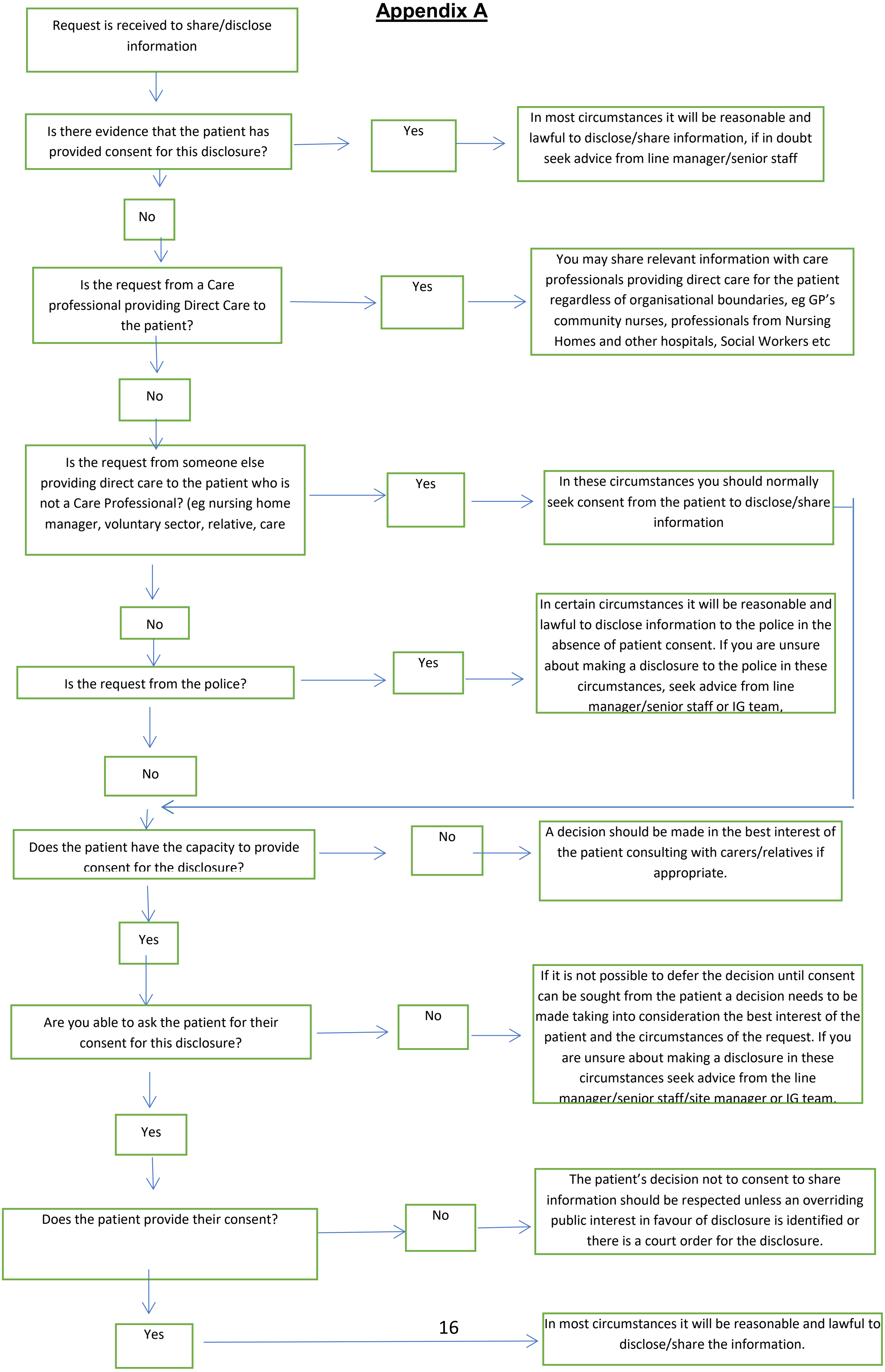
16.0 Definitions

Term	Definition
Personal data	Any information relating to an identifiable person who can be directly or indirectly identified
Data controller:	The organisation (in this case, the Trust) that determines the purposes for which, and the manner in which any personal data are, or are to be, recorded.
Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person or agency that processes data on behalf of the data controller.
Direct care	Provision of clinical services where interaction between the patient and a health care provider takes place. Examples include assessment, performing procedures and implementation of a care plan.
Duty of confidence	Arises when one individual discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.
Explicit consent	Consent normally given orally or in writing, where clear and positive indication is given that the individual understands what they are agreeing to. For data protection purposes, this must clearly set out how the information is going to be used and how consent can be withdrawn.
Information governance	A combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.
Legitimate relationship	A relationship that exists between a patient and an individual or group of individuals involved in their treatment which provides the justification for those users to access a patient record. Can also apply to staff records.
Processing	The collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to its alteration, retrieval, disclosure and destruction or disposal.
Non care or secondary purpose	Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

17.0 Related Trust Policies

- Health Records Policy
- Non Health Records Policy
- Disciplinary Policy
- Clinical Data Quality Policy
- Audio Visual Recording Policy
- Clinical Coding Policy
- Freedom of Information Policy
- Incident Policy
- Access to Health Records Policy
- Registration Authority Policy
- Network, Internet and Email Usage Policy
- Information Governance & IMT Security Policy

Appendix A



Request is received to share/disclose information

Is there evidence that the patient has provided consent for this disclosure?

Yes

In most circumstances it will be reasonable and lawful to disclose/share information, if in doubt seek advice from line manager/senior staff

No

Is the request from a Care professional providing Direct Care to the patient?

Yes

You may share relevant information with care professionals providing direct care for the patient regardless of organisational boundaries, eg GP's community nurses, professionals from Nursing Homes and other hospitals, Social Workers etc

No

Is the request from someone else providing direct care to the patient who is not a Care Professional? (eg nursing home manager, voluntary sector, relative, care

Yes

In these circumstances you should normally seek consent from the patient to disclose/share information

No

Is the request from the police?

Yes

In certain circumstances it will be reasonable and lawful to disclose information to the police in the absence of patient consent. If you are unsure about making a disclosure to the police in these circumstances, seek advice from line manager/senior staff or IG team,

No

Does the patient have the capacity to provide consent for the disclosure?

No

A decision should be made in the best interest of the patient consulting with carers/relatives if appropriate.

Yes

Are you able to ask the patient for their consent for this disclosure?

No

If it is not possible to defer the decision until consent can be sought from the patient a decision needs to be made taking into consideration the best interest of the patient and the circumstances of the request. If you are unsure about making a disclosure in these circumstances seek advice from the line manager/senior staff/site manager or IG team.

Yes

Does the patient provide their consent?

No

The patient's decision not to consent to share information should be respected unless an overriding public interest in favour of disclosure is identified or there is a court order for the disclosure.

Yes

In most circumstances it will be reasonable and lawful to disclose/share the information.