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

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.

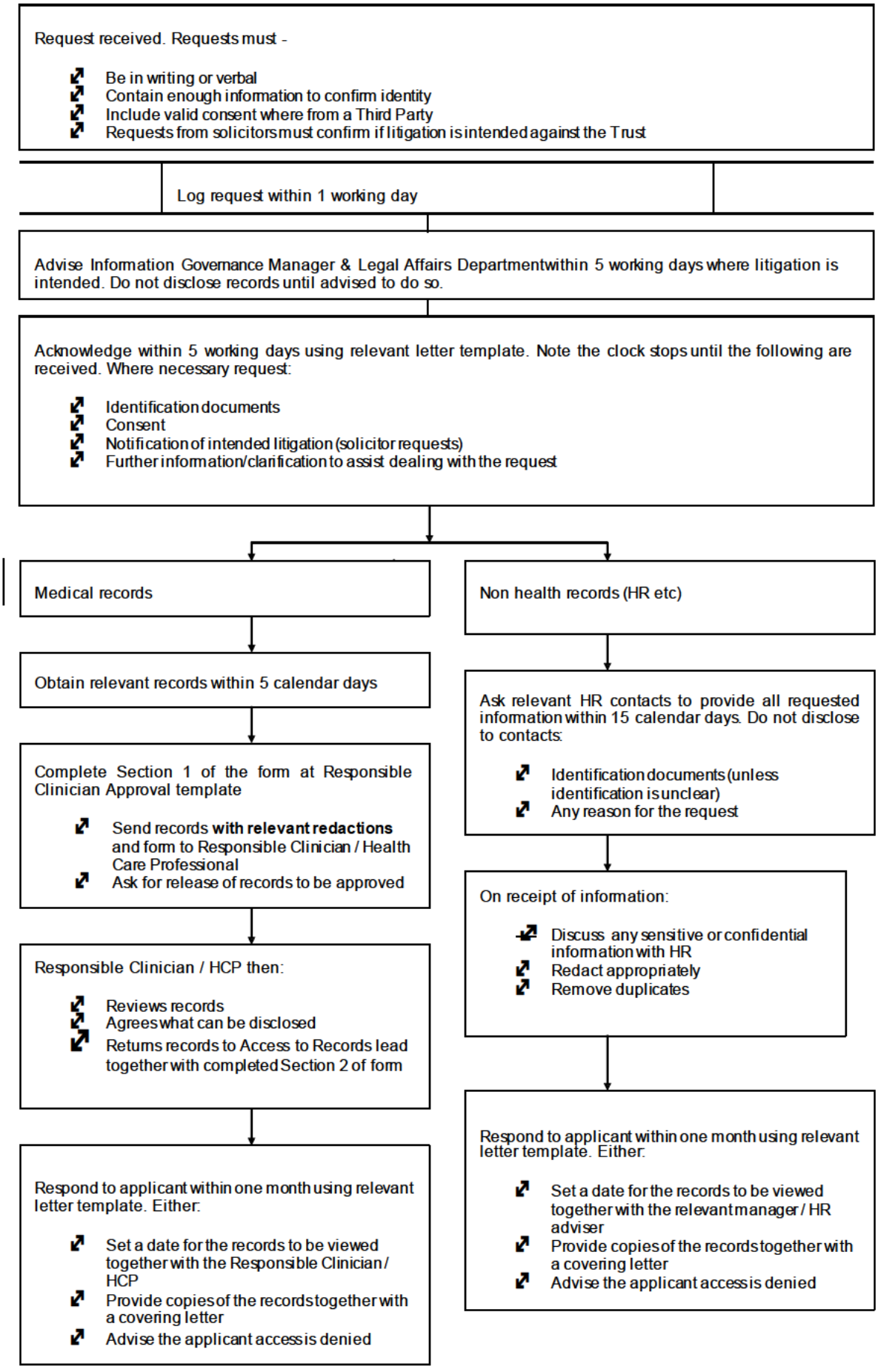
We do not use automated decision making to make any decisions about you.

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



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.

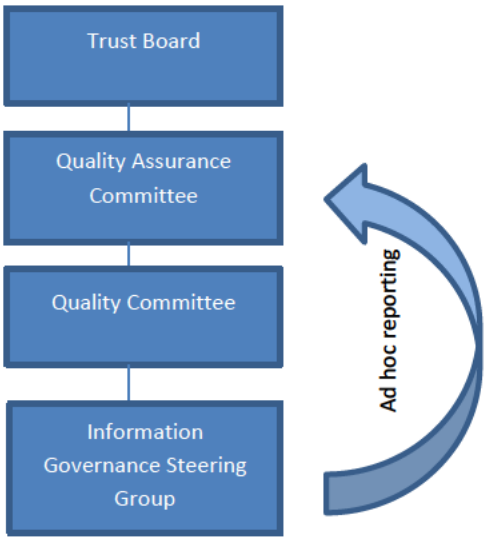
All users must sign a confidentiality agreement, either as part of their contract or as a separate
confidentiality agreement. Furthermore, individuals with privileged access to systems are required to sign an enhanced agreement to ensure they take their responsibilities seriously.

3.0 <u>Reporting structures</u>

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.



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.

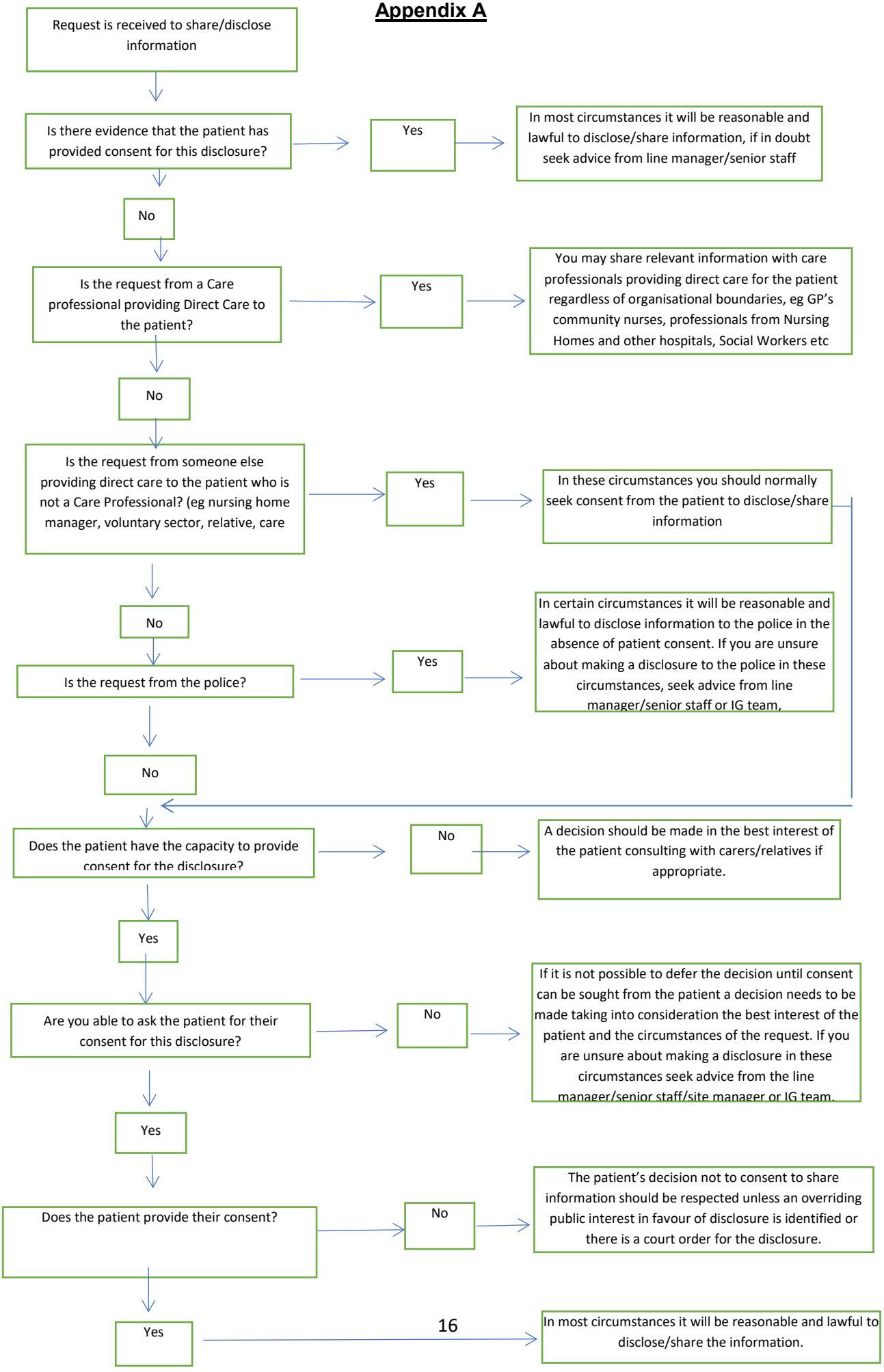
16.0 Definitions

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.

East London
NHS Foundation Trust

Patient Property Policy

(Incorporating the Key Safe Policy for community staff)

Version number :	3.0
Consultation Groups	Borough Lead Nurses
Approved by (Sponsor Group)	Borough Lead Nurses
Date approved	5th June 2024
Ratified by:	Quality Committee
Date ratified:	23rd October 2024
Name of originator/author:	Deputy Lead Nurse Lead Nurse Forensics
Executive Director lead :	Chief Nurse
Implementation Date :	October 2024
Last Review Date	October 2024
Next Review date:	October 2027

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

Version Control Summary

Version	Date	Author	Status	Comment
1	10th May 2018	Asha Sauboorah-Domah		
2	31 August 2018	Ruth Bradley & Caroline Ogunsola	Review and addition of community services practices	Approved July 2019
3	August 2024	Graham Manyere, Lorraine Greene and Matekenya Muzondo	final	

Executive Summary

The East London NHS Foundation Trust (ELFT) has established a policy to ensure the safe custody and management of patients' personal property during their care. This policy outlines the responsibilities of staff in handling both valuable and non-valuable items brought in by patients, particularly in inpatient settings and community care environments.

Key areas covered include:

- Admission Procedures: Guidelines for managing patients' belongings upon admission to wards and departments.
- Financial Management: Protocols for handling patients' money, especially during inpatient stays.
- Transfer and Discharge: Steps for managing property during patient transfers to other healthcare organizations or upon discharge to home.

For community-based services, the policy includes:

- Key Management: Instructions on the use of patients' keys and key safes.
- Allegations of Theft: Procedures for addressing claims from patients regarding missing property.

The policy aims to protect staff from allegations of theft and aligns with various professional codes and related policies, ensuring compliance with ethical and safety standards.

The Trust recognizes the diverse needs of patients, particularly those in long-term care, and emphasizes the importance of regularly reminding patients about property safety and secure storage options. Given the varying operations of different teams and wards, the policy encourages the development of localized procedures tailored to the specific needs of each service setting, while maintaining a consistent focus on safe property management practices throughout the patient's care journey.

Contents

Managing Patients' Property

1. **Introduction:**

East London NHS Foundation Trust (hereafter referred to as "The Trust") has a responsibility to provide safe custody for money and other personal property either handed in by patients or in the possession of confused patients or found to be in the possession of patients in our care. As a provider of long term care, the Trust also has a responsibility to provide a stewardship function for managing patient's property during their episode of care with the Trust. This policy explains how to deal with patients' property, both of a valuable and non-valuable nature while under the care of East London NHS Foundation Trust (ELFT). The Policy is designed to clarify the requirements of all staff members who manage the property of patients as part of their work within the organisation.

The security of patients' homes is vital in providing high quality and safe domiciliary care and community healthcare staff has a responsibility to ensure their actions do not place the security of patients, their families or their homes at risk.
This policy will therefore cover:

- Admission to wards and departments within the Trust
- Handling of patients' money especially whilst in an in-patient facility
- Transfer or discharge of patient to other health care organisations or non-health care organisations/home.

For staff providing community based services for housebound patients, Section 2 of this policy covers:

- Guidance on the use of patients' keys and key safes
- What to do when patient alleges that staff has stolen his/her property

This Policy will aim to protect staff from becoming compromised or subjected to allegations of theft and cross referenced to other related policies and guidance such as:

- Nursing and Midwifery Code of Ethics and Professional Practice
- HCPC Code of Professional Practice and Ethics
- Information Governance Policy
- Record Management Policy
- Resuscitation Policy
- Moving and Handling Policy
- Incident Reporting Policy
- Health & Safety Policy

2. **The Trust's Aim:**

The Trust aim to ensure the safe keeping of patients' property at all stages of their care and treatment; however due to the differing arrangements over how teams/ wards/units and services are operated to meet their patients specific needs, it is not possible to provide a definitive process or procedure.

It is also important to recognise that patients may be within ELFT units and wards for significant periods of time and as such there will be changes in the property that they originally brought in. Furthermore because of the long term nature of some patient/service user admissions, they will tend to regard their "room" as "home" for the duration. As such they may seek to bring personal property and items. Staff must remind patients over the need to keep items safe and

to use safe keeping facilities; this message must be re-iterated periodically. The principal concern of the Trust is the demonstration of safe practice when managing patient property within ELFT and on transfer to other health care settings not part of ELFT. Local documented procedures specific to the service setting or unit should focus on the complexities of the individual clients under the Trust's care, such as in Learning Disability units or community based services.

3 Who does this policy apply to?

3.1 This policy applies to all staff working in services under the umbrella of East London Foundation NHS Trust (ELFT). However, local services may draft local procedures to suit their client base and practices but this must be compliant with this Trust overarching policy.

3.2 ELFT will expect other services that use the organisation to also apply the principles of this policy as a minimum standard within their service.

3.3 With respect to minors, or patients/clients who lack mental capacity, the policy will apply to those identified as having the guardianship or legal power e.g. Power of Attorney. The Power of Attorney must be checked with the Office of the Public Guardian before handing over property of value.

4 Definitions

The use of the term "property" shall be taken to include money, valuables, keys, medicines and personal belongings.

Cash - money in the form of coins or notes as distinct from money orders or credit.

Cashier – this is the Trust department that manages patients' finances. Cashiers provide robust accounting processes to manage patient finances and should be used wherever possible.

Valuables – items having significant monetary value; having great importance or usefulness; cherished or esteemed because of personal qualities; capable of being assigned a value for example - a possession, especially a piece of jewellery - that has significant monetary value.

Non Valuable /Personal possessions – items owned by or for the personal use of the patient, other than those which are considered valuable, illicit substances and risk items – this term covers items which may be in the possession of the patient on arrival at the ward/unit; that they may bring to the unit following a period of leave or which has been brought in by a friend or relative and which may be harmful to their or other patients' safety and consequently must be removed from the patient, for example knives; sharp items or possible ligature risks. Illicit substances such as controlled drugs will be handed to the police for destruction and a receipt must be given to the patient. However, do not report small amounts of illegal substances to the police as, on balance, the duty of confidentiality outweighs the misdemeanour of possession.

SECTION ONE

5. General principles

5.1 In inpatient facilities, disclaimer notices must be displayed in conspicuous areas accessible to patients and their relatives, to ensure that they are clear on the Trust's stance of property safety and storage.

5.2 The disclaimer notice and disclaimer form and the wording within should be brought to the attention of the patient and recorded in the patients notes and where possible upload in their respective files on RIO / EMIS / SystmOne (Appendices 1 and 2).

5.3 If staff fails to obtain a signed disclaimer and the property remains with the patient, the organisation could be liable for loss, due to negligence.

5.4 It must be assumed that all patients have the capacity to make a decision about the safekeeping of their property; if it is deemed that a patient does not have the mental capacity to make that decision, staff must follow procedures in assessing and recording capacity in line with the Mental Capacity Act (2005).

5.5 All Property must follow the patients in their journey through the episode of care.

5.6 Use of terms such as 'gold' and 'silver' must not be used when describing items of jewellery. Descriptions such as 'yellow coloured metal' or 'white coloured metal' must be used instead.

5.7 Stones in rings or other jewellery must not be described as 'diamond', 'ruby' etc. but the terms 'white coloured stone', 'red coloured stone', must be used.

5.8 Only one property book or list, and valuables book should be in use at any one time in an area. These items should be treated as controlled stationery and consecutively numbered or referenced. This should include subsequent lists raised listing property and then these should be cross referenced.

5.9 The wards or Patient Welfare officer are responsible for retaining completed books in accordance with Organisation policy for a period of six years.

5.10 If the patient is unable to look after their property due to illness or lack of capacity for any reason, money, valuables and house keys should be retained by the Trust until patients have recovered sufficiently to give instructions as to their safe-keeping.

5.11 If patient's property is returned to a relative or carer at any time during the patient's stay within the hospital or unit, a receipt that includes a list of all the property returned is required. This will make it clear what has been returned to minimise dispute at a later stage and must be obtained and stored in patient's notes.

5.12 This is especially in relation to keys, money, jewellery and other valuables, dentures, hearing aids or other similar medical devices. If the patient has capacity then the instructions and documentation must be signed by the patient. It would also be beneficial to have a Multi-Disciplinary Team (MDT) input in these discussions.

6. Training requirements

6.1 There are no specific training requirements for this policy; however all staff must be advised of local procedures at local induction in relation to how to deal with patient's property (valuable and non – valuable) keys and monies.

6.2 This should be recorded in the Local Staff Induction Pro-forma and be signed off by the manager to confirm the induction took place.

6.3 Failure to follow local procedures must be managed by the manager or a senior staff member; ensuring that the correct procedure is shared and understood.

7.0 Duties and responsibilities:

7.1 Chief Executive:

The Chief Executive has ultimate responsibility for the management of security and safety of staff and service users in the organisation. This responsibility also includes ensuring the aims and objectives of this policy are met, and ensuring that adequate resources are made available for the implementation of the policy.

7.2 Service Directors/Associate Directors/ Heads of Service/ Departments & Matrons/Specialty Managers:

It is the duty of these group of senior managers to raise staff awareness to this policy; and that there are robust local procedures for the management of patient' property for areas/units under their control and for providing the necessary resources to ensure that the processes are followed.

7.3. Clinical Leads / Ward managers/Unit/Locality Managers:

It is the responsibility of the Clinical lead /Ward Manager/Unit/Locality Manager to ensure that:

- Robust local procedures for the management of patient' property that meet the general requirements and principles of this policy for areas under their control are in place and that all staff are aware of them.
- Necessary resources are provided to ensure procedures are followed
- Staff members discourage patients from retaining cash and/or valuables and that relatives are also discouraged from bringing in cash and valuables. Where cash or valuables are brought into the Ward / Service, they are disclosed to staff so that they can be held in safe custody
- A Disclaimer Notice is placed in visible areas on the Ward's Notice board for relatives to sight. (See Appendix 1).
- They provide safe custody of keys, money, valuables and other personal property, which is:
  - handed in by patients;
  - in the possession of unconscious or confused patients;
  - Found in the possession of patients dying on admission to hospital.
- The ward manager is responsible for ensuring that regular audits are undertaken to meet the needs of the service [minimum quarterly] and ensure that the contents of the ward safe match the documented lists of items held for safekeeping/patients property lists.

- The audit should be documented and retained as an electronic document – hard copies may be stored within the safe. Where no property is held on behalf of patients, then this should be clearly documented.
- They are also responsible for ensuring that any deviation or errors arising, including losses or discrepancies are dealt with in the correct and timely manner.

7.4 Nurse in charge:

The Nurse in Charge of the shift /team/unit is responsible for ensuring:
That the Patient Property Lists and Disclaimers are completed on admission of the patient and that all cash is counted in the presence of the owner and another colleague.
That nursing staff should liaise with the Patient Welfare officer or Cashier with regards to any patient who may be approaching discharge or potentially being transferred to another unit to enable them to ensure that their money/ valuables will be available to be released with the patient.

7.5 Nursing staff:

It is the duty of the admitting registered nurse to advice patients to:
- Send property home whenever possible
- Inform Nurse in Charge when additional valuables are brought into hospital
- Complete the disclaimer form and refer them to the disclaimer notice.

7.6 All staff:

All staff have the responsibility to:

- Follow the guidance in this policy and local procedures and should not hold patients' monies or property in their care.
- Be aware that there are very strict rules over the handling of patient monies / valuables and these must be followed at all times to prevent loss or for staff to become compromised and potentially subjected to investigation and possible disciplinary procedures.
- Know the location of property taken into safekeeping and ensure that this is recorded and communicated to other health care professionals throughout the patients' stay.
- Escalate concerns where a patient is known to have possession of cash or valuables that have not been handed over for safekeeping or where cash and valuables have recently been brought to the ward/unit by a friend or relative. If the client refuses to place valuables into safe keeping, the disclaimer form should be completed.
- Where the reason for any loss cannot be immediately identified, this should be referred to the **Trust's Local Security Management Specialist** for advice or investigation and the **Trust's Legal Services Manager** should be informed. The incident should be reported on the In phase system and recorded in the Patients notes – RIO / EMIS/ SystmOne.
- Staff have a responsibility to empower patients and service users and to help them to manage their money; however decisions over how a patient spends their money is theirs and staff should not tell a patient what to spend money on, or not.

7.7 Patient Welfare Officer:

A Patient Welfare Officer is employed to provide a support role to patients and their relatives during a hospital stay. In this policy and throughout these procedures the officers will be referred to as the Patient Welfare Officer (PWO). Where no PWO is employed, the Cashier will take on the PWO responsibilities where appropriate **(See Appendix 4**).

7.8 Cashiering Arrangements:

- Ward Staff should advise patients that access to their personal expenditure is via the Cashiers office. This is obviously restricted to the following opening hours.

City & Hackney Centre for Mental Health:	**13.00 – 16.00 Mon to Fri**
Centre For Forensic MH:	**09.00 – 13.00, 14.00 – 16.00 Mon to Fri**
East Ham Care Centre:	**14:00 – 16.45 Mon to Fri**
Newham Centre for MH:	**09.00 – 12.00 Mon to Fri**
Tower Hamlets Centre for MH:	**08.30 – 11.30 Mon to Fri**
Wolfson House (Forensic):	**09.00 – 13.00, 14.00 – 16.00 Mon to Fri**
Luton (ECT Unit):	**10.00 – 14.00 Wed & Thurs**
Archer Unit Bedford	**24 hours access to nursing team for safekeeping.**

- Staff should make the patients aware that the PWO advises the Cashier on recommended daily allowances for each patient depending on their benefits and balances. Staff should try to support the Cashier and PWO in these matters.
- Staff wishing to withdraw money on the patients' behalf must use the appropriate Staff patient Money form or Property Request form. This is used only when the patient is unable to attend the Cashier in person.
- The patient has to sign the form on the ward and it has to be authorised by the nurse-in-charge. Another member of the ward staff needs to take the completed form to the cashier for payment.
- Any patient wishing to withdraw cash from the Cashier must have a member of the ward staff who will act as an escort to witness the withdrawal.

8. Local Security Management Specialist (LSMS)

The Local Security Management Specialist (LSMS) take forward security Management work locally in accordance with national standards. The LSMS will work with key colleagues to promote the secure management of patient's property and effectively respond to incidents and security breaches relating to patients property.

9. Local Counter Fraud Specialist (LCFS)

The Local Counter Fraud Specialist can investigate fraud affecting patients' money and valuable property but is not responsible for investigating the theft of patients' monies.

10. Management of Patient Property – Process For All Patients

10.1 Classification of Property

Patients' property can be broadly classified into two types:
• Patients valuables, including monies or cash equivalent property, bank and credit cards, cheque books, Passport, Home Office document, EU ID Cards, National Insurance Card,

Driving Licence, birth certificates, jewellery, wrist watch, portable and handheld electrical goods, smart phones, laptop & tablets, keys etc.

- Patients Clothing, including, shoes, belts, hats, caps suitcases, handbags, dentures, spectacles etc.

10.2 Handling of property on admission

10.2.1 Patients should be advised to bring only minimum amounts of property and valuables into hospital. Where excessive amounts of property are brought into hospitals or property accumulates, and then relatives should be asked to take excess property home in order to keep minimal amounts of personal effects in our units. This must be recorded in the property book and would apply to both valuable and non-valuable items at all times. The relative's name must be recorded and a date and time of the removal also be inserted. The relative should confirm receipt of any items of value or cash in writing.

10.2.2 Patients should be advised in all admission letters that valuables, cigarettes & lighters should not be brought into hospital while on admission.

10.2.3 Where this has not been possible, e.g. in the case of emergency admission or detained under section, patients should be advised to have valuables taken home as soon as possible by a relative, carer or friend; otherwise they can deposit money or valuables which are not immediately required into the organisation's safekeeping e.g. Cashiers.

10.2.4 Where the patient declines to hand over their property and where a disclaimer is signed, the Organisation cannot accept liability for any loss incurred. Where a patient refuses to sign a disclaimer this must be noted on the disclaimer form by the staff and signed by two members of staff.

This should also be brought to the attention of the ward manager. Staff should make every effort to ensure that the patient's relatives and/or carer are aware that the patient has refused to sign the disclaimer and explain that the organisation is unable to take responsibility for cash or valuables.

It is not appropriate for a relative to sign the disclaimer on behalf of the patient. In circumstances where patients are unable to safeguard their valuable property kept on them, staff should take the items away for safekeeping. Again this decision should be documented in patient's own record.

10.2.5 Where valuables are held at ward level this must be for the shortest possible period of time.

10.2.6 Where property/valuables are being held by Cashiers, they **must be** informed when patients are transferred between wards or discharged.

10.2.7 Normally, property should not be handed over by the Organisation to third parties without the consent of the patient, but personal articles of small value and clothing may be handed to their relative or carer and a record kept as good practice with names dates time inserted along with person's relationship with patient. Staff should ensure that the person receiving the property is either a known relative or identified by the patient as being suitable to receive property. Proof of ID should be obtained and a signature provided prior to property being handed over.

10.2.8 If the patient is not able to consent, or take responsibility, to property being released and the ward staff have doubts about the eligibility of the person collecting property, they must arrange for it to be stored in safekeeping until eligibility has been confirmed.

10.2.9 Staff to consider taking pictures of all the items that the Trust is holding for patients and upload onto the respective files on RIO/EMIS/SYSTMONE and give the patient a copy of the picture of their belongings.

10.3 Handling and management of patients' money / valuables

10.3.1 Patients may be vulnerable and supporting them with the management of their finances and money should be considered as part of the care plan. There are very strict rules which must be followed in managing patients' finances. See Appendix 3 for "do's and don'ts".
Under no circumstances should staff make withdrawals or purchases on behalf of a patient using the patient's bank card. Patients should never be asked to disclose their PIN. This applies to all staff that looks after in-patient settings, out-patient clinics and patients in community settings.

The Patient Welfare Officer & Cashiers manage patient monies and have clearly auditable processes which, when followed protect staff from possible allegations of fraud or misconduct.

10.3.2 Each service will put in place local processes to enable patients have access to their funds; however where a Cashier is available, use of this must be encouraged as this process offers significant safeguards to prevent staff from becoming compromised.
Local processes and procedures must meet requirements of this policy, auditable and these should be made available to patients in order to help them manage their finances. Just as we encourage and support patients to manage their own medication, care plans should include appropriate support for each patient to assist them in financial management wherever necessary.

10.3.3 Some patients may be very unwell on admission and care must be taken to ensure that any cash that is brought in with them is counted and a record made of the total.
Where a patient does not have capacity the money must be counted and for this to be witnessed by a second member of staff and deposited with the Cashiers and this recorded until the patient is able to make decisions.
Where the Cashiers is inaccessible for out of hours, then money should be sealed in an envelope and held in the ward safe. The envelope should be sealed by signing over all seals where the folded envelope meets the body of the envelope and then placing cellotape over the signature and joins. This must be documented in the patient's records.

10.3.4 Services may have a daily or weekly limit for patients making withdrawals; however some patients may require a smaller personal limit, for example where a patient is known to be reckless with regards to management of their finances. This may be discussed and agreed by the multi-disciplinary care team.

10.3.5 Visitors should be encouraged to advise staff if they have given cash to a patient so that where there is concern for the patient's financial management, it can be deposited with the Cashiers for safekeeping.

10.3.6 Where patients use personal money to make purchases then they should be encouraged to retain receipts where available. Patient must be encouraged to make their own purchases when on leave or encourage family members or visitors to bring items that they need or intend to buy in to the ward or hospital for them.
Under no circumstances should staff use their own money to purchase items for a service user / patient.

10.3.7 In exceptional circumstances where a patient may not have immediate access to funds and as a last resort, a loan may be granted from Petty Cash from the ward or an advance given by the Welfare dept.

The loan should be for a minimal amount, as agreed based on the patient circumstances. This must be documented and a signature obtained from the patient. Please refer to the Petty Cash Guidelines on the Intranet.

10.3.8 Where the Local Authority has an "appointee ship" for an ELFT service user then this policy and local arrangements will be followed in respect of managing the patients' money. For Department of Works and Pensions appointee ship the Trust is the appointee with a named person acting on their behalf. This is a finance role conducted by and carried out by a named person. No other members of staff must take on this role as it's a formal responsibility and must be exercised according to Trust policy.

10.3.9 Decisions over family and friends involvement in any patients' affairs should be made in consultation with the patient. Many patients will have valid reasons for not wanting their family or friends involved in their financial decisions and this should be considered and where appropriate respected. Any decision to share information with regards to a patient's family/carers must be clearly documented together with the rationale for doing so.
10.3.10 Where the ward/service has retained monies and/or a valuable item/s on behalf of a patient, e.g., in a ward safe, there has to be an accurate record kept of where/when the items have been signed in/out. Two members of staff or a patient and a staff member should always sign.

10.4 Reporting Losses of Patient Property

Staff are to be mindful of the potential for Identity Theft related to phones, tablets, Passports or any other forms of Photo Identifications.

10.4.1 Loss of Cash: In all incidents where it has been brought to the attention of any member of the ward team that there has been a loss of cash this will immediately be escalated to the Registered Nurse in charge of the shift who will:

- Instigate a search of the ward area to ensure that the money has not simply been mislaid
- Report the loss to the Police via the Emergency services non –urgent number 9 101 without delay and **no later** than by the end of the shift.
- Obtain a CAD number from the Police.
- Ensure an In phase is completed no later than by the end of the shift and the CAD number is recorded.
- Inform the patient & ensure that the RIO / EMIS record of the patient indicates the loss and confirming the actions taken.
- Inform the relatives where appropriate of the loss and the actions taken.
- Inform the Duty Senior Nurse / Clinical Lead of the loss and confirm that the appropriate actions have been taken.
- Inform Richard Harwin – The Trust Health, Safety, Security and Emergency Planning Manager with details of loss together with CAD number obtained from the police.
- Inform the lead nurse and the Modern Matron and confirming that the appropriate actions have been taken.
- If out of hours, inform the on call Manager who will give further directions.

10.4.2 Loss of valuables retained by a patient:

All incidents of loss of a valuable item that have been brought to the attention of a member of the ward team by patients':

- Relative
- Visitor

- Any other source

The same reporting pathway and time frames as that for the loss of cash should be followed in this circumstances.

10.4.3 Loss of Personal items

Any occurrence of loss of personal items must follow the same reporting pathway as above. However, *there is no need to report such items to the police or to obtain a CAD number*. An In phase will still need to be completed to provide information and evidence and an audit trail to examine and adjust ward systems to reduce further occurrences.
Examples of personal items include but not limited to:

- Dentures
- Glasses
- Clothing
- Toiletries

10.5 Medicines Management

10.5.1 Medicines brought into hospital remain the property of the patient throughout their stay. This would be for prescribed or purchased medicine.

10.5.2 A record should be kept of all medicines brought into hospital by the patient

10.5.3 Medicines should be kept in safe custody within the ward,

10.5.4 Verbal consent for their use or destruction during the hospital stay must be obtained where it is in the best interests of the patient.

10.5.5 If a patient dies while under our care, any medicines brought into the hospital by the patient should be returned with other property to the next of kin.

This does not apply to Controlled Drugs which should be destroyed by a person with the authority to do so. Please see the Controlled Drugs policy for further guidance. Technically CDs are part of the deceased person's estate so the next of kin can ask for them – however this should be discouraged and they should be made aware that it may not be legal for them to possess.

10.6 Discharge or Transfer

10.6.1 On discharge or transfer, the outgoing property should be cross referenced against the Record of Patient's Property which was completed on Admission and against any other additional property record that has been completed over the course of the patient's stay.

10.6.2 Ward staff will inform the PWO in advance if a patient is going to be discharged and the PWO should liaise with the ward staff and the Cashier to ensure that any valuables are returned, prior to discharge.

10.6.3 The PWO should ensure that they check the discharges weekly either on Rio / Systmone (electronic patient registration system) or by getting a list of discharges from medical records.

10.6.4 The PWO is responsible for returning cash to a discharged patient. This can be in the form of cash or cheque, depending on the value and how much cash the cashier has available.

If a cheque is to be drawn, the PWO should complete a Request for Patient Monies (RPM) and pass this to Finance for processing.
The PWO should ensure that a forwarding address is given if the cheque is not available prior to discharge. Should the patient not have a bank account to deposit their cheque in, cash can be ordered and paid to the patient with permission from the Financial Accountant.

10.6.5 The PWO should ensure that DWP payments into the Trust bank account are stopped once the patient is discharged. Alternative payments can be made to the patient on discharge, through a post office card account or through their own personal bank account.
If the patient is unavailable or unwilling to sign the DWP letter/fax regarding change of payment method, the PWO may write to the DWP advising them that as the patient has been discharged, it is no longer appropriate for their benefits to be paid into our Trust bank account and that the patient would contact them to rearrange their payments.

10.6.6 Patients discharged from hospital can reclaim any property held by the hospital for safekeeping, by producing their receipt, given to them at the time their property was handed in.

10.6.7 On transfer of patients between wards in the same hospital, where valuables are already in custody in a Cashier's office, the transferring ward are responsible for informing the Cashier and the receiving ward.

The property book must be updated to include where the patient is being transferred to. A copy of the patient's property form should be made and passed to the receiving ward.
Receiving ward should treat the arrival as a new admission. This will help to prevent any disputes and protect staff.

10.6.8 A Cashiers Property Register must be signed by the person collecting the valuables from a cashier. Staff collecting valuables and returning them to patients must ensure that the patient signs the Ward Property/Valuables Book. Staff should check the property they are receiving to ensure that it is correct before returning to the patient.

10.6.9 Where it is known that a patient is due to be discharged at a weekend or a bank holiday, a Cashier should be contacted in advance to ensure that arrangements are made for the property to be obtained prior to the date of discharge.

10.7 Death of the patient:

10.7.1 On Death where there is a known Next-of-kin

- If the value of the cash held by the Trust is less than £5000 then the PWO should return this to the next-of-kin. If the Trust has organised the funeral, the PWO should deduct the cost of this from the estate. The PWO should ensure that an "Indemnity Form" is completed and signed by the next of kin before raising a RPM for the Finance department. If the amount is £5.00 or less, this can be obtained from the cashier with the completion of the "statement of refund of patient monies".

- If the value of the cash held is more than £5,000 (after funeral expenses if applicable) then the PWO should ensure that Letters of Administration are obtained from the court, before completing a RPM. A cheque will raised payable to the person named on the Letters of Administration

- Other property should have been forwarded to the PWO from the wards and this should be returned to the next-of-kin. The PWO should ensure that the next-of-kin signs for

the property and if no Letters of Administration are issued, an Indemnity Form needs to be completed for property also.

10.7.2 On Death Where There is No Lawful Kin

- If a patient dies intestate and is not survived by lawful kin, then the estate of the deceased belongs to the crown. Reasonable funeral expenses can be charged to the estate and the PWO is responsible for organising this. If the balance of the estate is more than £500 the PWO should refer the matter to the Treasury Solicitor. Details available on the website: www.bonavacantia.gov.uk/output/Referring-Estates-To-The-Treasury-Solicitor.aspx. Every effort must be made to ascertain the details required by the Treasurer Solicitor.

- If the balance of the estate is less than £500 then the matter should not be referred to the Treasury Solicitor. Instead, the PWO should advise the Financial Controller in writing, attaching appropriate paperwork, and confirmation will subsequently be given that the individual patient record can be closed and archived by the PWO

- If after funeral expenses the patient estate is in deficit, then the PWO should inform the Financial Controller in writing with all the relevant details, and request that the debt is written off. This should be authorised by the Service Manager for Mental Health. Confirmation will subsequently be given that the individual patient record can be closed and archived by the PWO.

10.7.3 It is the responsibility of nursing staff to inform the PWO / Cashier, as soon as possible upon the death of a patient, for whom valuables are being held.

10.7.4 Nursing staff must not write 'RIP' or 'deceased' on property books as they may be seen by relatives. This should be left blank.

10.7.5 If the deceased person is removed by local funeral directors, property left on the patient must be checked and signed over to them before the body is removed from the ward

NB this will not apply to all hospital sites where there is not a cashier or hospital safe available – please refer to local procedures.

10.8 Funeral Arrangements and Expenses

- Next-of-kin will normally make the necessary funeral arrangements for a deceased patient. Payments for **basic** funeral expenses can be made from the cash held on behalf of the deceased patient (maximum £3000), provided receipts are produced by the person making the arrangements and an Indemnity Form is signed.
- The PWO should arrange the payments by completing a RPM form that should be forwarded to the Finance department.

- When a patient is admitted without a notified next-of-kin, the PWO should make all reasonable attempts to locate them. If this proves unsuccessful and the patient dies, the PWO should arrange for burial using local undertakers. In order to ensure value for money the PWO should obtain two quotations before booking the funeral.

- The cost of the funeral should be met from the deceased patient's property balance. If there are insufficient funds held by the Trust and no next-of-kin or relatives can be located the PWO should proceed with the burial arrangements and liaise with the Deputy Director of Finance to sort out the funding arrangements.

10.9 Procedure for dealing with property taken into safe keeping

10.9.1 Property handed over for safekeeping must be examined, recorded in the appropriate property book or list and signed for by two members of staff. A signature should be obtained from the patient (where possible) to acknowledge the list of property handed over for safe custody is complete and correct. Details of any action taken must be documented in the patient's records, (including any patient's refusal to sign), and must be witnessed by two members of staff.

10.9.2 In the case of clothing, all items should be placed into an appropriate bag and a copy of the Property List attached, clearly identifying the patient's name, hospital number and ward. The bag must be stored in a secure area in the ward or department. Wherever possible, the clothing list must be cross referred to the property book entry.
In the case of valuables, a separate page must be used for cash, and for other valuables, as these could be lodged in different locations.

10.9.3 When recording valuables, the following details should be noted:

- Social Security Cards and Card Numbers.
- Credit Cards the type of card e.g. Barclaycard or MBNA and the last four digits of the credit card number.
- When recording keys the number of keys should be noted.

In the interest of security the credit card number [16 digit number across the centre of the card] and the security number on the back must not be recorded

10.9.4 All valuables must be placed in a suitable envelope with the copy of the property list and sealed as described before. Neither the details of contents nor the copy of Property List attached or recorded on the front of the envelope. The envelope must also record the page number from the Valuables Book, if applicable. The signature of the two members of staff, who have checked the contents, must then be recorded on the front of the envelope and over the seal.

- Where provided, property should be stored in a sealed tamper proof bag. The seal number is recorded on the property form. Where access is gained to the bag, the new seal number is added to the property form and reason for the access recorded. Should these not be used, then the upper envelope seal and the lower enveloped seal should signed by the staff. Cellotape is then place over the seal and the staff signatures. Staff then should initial the edge of the Cellotape. This will identify any attempt to gain unauthorised access into the envelope.
- Where property is required to be accessed and some property removed, then a new envelope is used to store the remaining property and sealed in the above manner. A list of the property should then only be included within the envelope and the original envelope should be retained with the property with the reason for the access to the property recorded on it.

10.9.5 Patients must be advised that any property lodged with a Cashier, if applicable, may not be accessible at weekends or 'out of hours'.

10.10 Property/Valuables during Office Hours

10.10.1 Where cash, credit cards, cheque books, jewellery etc. are involved, the Staff members involved in the checking process will ensure that they both take the sealed envelope to the Manager's office, deposit it within the 'Ward drop Safe', both signing the 'Safe Log Book' to confirm that one sealed package has been deposited. **It is individual ward responsibility**

to notify the welfare officer that there are items in the ward safe needing transfer to the Cashier's office.

The Patient Welfare Officer will ensure that:

- Valuables are transferred to the Cashiers office as soon as is reasonably possible and in all cases no later than within 24 hours of a weekday admission; and where admission takes place at a weekend or public holiday then at the next working day.
- Ward Deposit Safes are only opened in the presence of the Individual Ward Shift Coordinator.
- The Safe Log Book has been appropriately signed by both parties.
- In the absence of a Welfare Officer it is the Ward's responsibility to advise the Duty Senior nurse / Matron that there are items that need to be transferred to the Cashier. It is the responsibility of the Duty Senior Nurse / Matron to ensure that the items are treated as above.

10.10.2 The receiving person will sign the book/list on behalf of the Organisation, accepting responsibility for its safekeeping. The receiving person will retain a copy of the list and attach this to the envelope. The member of staff will return a signed copy to the patient and keep a record in patient's notes.

10.11 Transfer of Property/Valuables out of Office Hours

- Where patients are capable of caring for their own property, the receiving ward must ensure that a further disclaimer form has been signed.
- Outside office hours and during weekends, valuables should be dealt with as below: The following procedure should be applied:
- All Cash is entered into the Patients Property/Valuables Book/Property List and put in a sealed envelope and signed by two members of staff. As per NB to paragraph 8.9.4
- Valuables, including chequebooks, credit cards etc., are entered into a different page of the Patients Property/Valuables Book/List and placed in a separate envelope
- The property should be transferred on the next working day to a Cashiers Office if available, or stored immediately in a safe location.

10.12 Special Circumstances

10.12.1 Temporary custody of property and valuables should only be undertaken on wards and departments as a short-term measure, e.g. patients attending procedures or theatre, until their property and valuables can be returned to them or their relative or carer.

10.12.2 In all cases the temporary custody section of the Property and/or Valuables book/List **MUST** be completed and the property lodged in the department's designated secure location, e.g. this may be the ward safe (valuables should be held for the shortest time possible and no longer than 24 hours)

10.12.3 Where property is already in custody the receiving ward must treat it as a new admission and also sign off the original ward's book or list as having received the property.

10.13 Documentation

10.13.1 Each ward/department should only have one valuables and clothing book in use at any one time. To be treated as controlled stationery and to be properly referenced

10.13.2 Pages must be used sequentially.

10.13.3 Completed Property or Valuable Books/copies of lists are retained by the ward for six years.

10.13.4 Patients Valuables Book should be used; these are in triplicate with the distribution of copies as follows:

- **Copy 1** – given to the patient. If the patient is not able to receive this copy it should be retained with the patient's medical records until such time as they or their relative or carer is able to receive it.

- **Copy 2** - Accompanies cash and valuables and is retained by the Cashier.

- **Copy 3** - Retained in book.

10.13.5 All spoiled copies are to be retained in the Patients' Property/valuables or Clothing Book and clearly marked 'Cancelled', an explanation for the cancellation written and signed by the author. Two distinct lines should be drawn from the top to the bottom of the page and the words '**ERROR**' be written across the page and the reason added and signed by the author.

10.13.6 In accordance with the Organisation's Standing Financial Instructions staff should be informed at local induction with regards to their duties for the administration of patients' property and for the training to be documented.

10.14 Unclaimed Property

10.14.1 Every attempt must be made to reunite property with the rightful owner. However, after a period of 6 years, following discharge or death, unclaimed property will be disposed of. Care should be taken to ascertain whether articles are of value and expert advice sought where there is any doubt about the value. Where property includes bank cards, the issuing bank/building society must be notified and may act as a source to trace the account owner's location/address. Bank cards must be destroyed rather than being retuned by post. The Cashier /Welfare officer will destroy cards by cutting them into at least three pieces or by shredding and for this to be witnessed by another staff member. Record the action that has been taken to provide a complete audit trail. Destroying the card[s] will avoid any possible misuse of the card.

10.14.2 If there are unclaimed articles of value, reasonable efforts, which should be recorded along with dates and times, should be made to trace the owner. This may include, but is not limited to, making contact with the patient's GP for a new address; contacting any known next of kin; conducting a "google search" for possible electoral role registration or contacting local Social Services.

If the trace is unsuccessful the articles should be kept for a reasonable time before disposal. Under the Limitations Act 1980 a period of six years would normally be reasonable in the case of property deposited although this period of recovery may be extended in the case of disability acknowledgement, part payment, fraud and mistake.

10.14.3 Unclaimed cash and the proceeds of the sale of abandoned or unclaimed property should be credited to a control account. In the event of a patient or some other person eventually claiming property which has been disposed of, the amount due would be payable out of this account; this will be arranged through the Finance Department. If selling property at least three valuations from reputable dealers should be sought. This will assist in showing that the Trust has been diligent in its dealing with the property. Lost property book should be

updated to state what has happened to the property and where any value and proceeds of sales are held.

10.14.4 All unclaimed bank books should be forwarded via the Organisation's Financial Services Department to the appropriate bank/Department of Works and Pensions office, with an explanation of the circumstances in which they came into the Organisation's possession. Ward/Unit property books should be completed to reflect this and the property signed for by a member of staff at the Finance Dept.

10.14.5 All unclaimed cash and valuables that exceed £500 held on behalf of a deceased patient will be forwarded to the Treasury solicitor by the Financial Services Team once all efforts by the ward and financial services to trace relatives have failed.

10.14.6 Where money is held on behalf of patients, it should be held either by the patient's affairs office or in the patient's own care. If it needs to be stored in exceptional reasons on the ward it must be returned to the patient or patient's affairs officer as soon as possible.

10.15 Handling property for patients who lack capacity

10.15.1 Where a patient lacks capacity to make a decision about their property, staff may have to make the decision in their best interests. This must be done following the requirements of the MCA and the related Code of Practice. Where staff have a reasonable belief that a patient lacks the capacity to make a particular decision about their property (e.g. handing certain items to the organisation for safekeeping), they should consider whether everything has been done to help and support the patient to make the decision; and whether the decision needs to be made without delay, and if not, whether it is an option to wait until the person has the capacity to make the decision for himself or herself (e.g. where the patient is under the effect of medication).

10.15.2 Staff should bear in mind that if a patient lacks capacity to make a certain decision on one occasion, that does not mean that they lack capacity to make another decision on the same or a different matter, or that they will lack capacity to make that decision in the future.

10.15.3 Provided certain conditions are met, staff may be protected from liability for carrying out actions in connection with the care and treatment of patients who lack the capacity to consent. The conditions relate to compliance with the principles of the MCA and with requirements around assessments and best-interests decision making. Actions taken by staff to protect a patient's property can be considered to be related to their "care and treatment", and may thus be protected from liability. The MCA does not, however, protect staff from liability for negligence. Therefore if staff places a patient's property into safe custody in line with the MCA, but then is negligent in handling it, they will still be liable for any loss or damage that occurs.

10.15.4 The most common action staff may consider taking in relation to a patient's property when the patient lacks capacity to make a decision with regard to it is taking the property and placing it into safe custody, thus meeting the NHS organisation's obligations and duty of care. Before doing so, staff should consider whether there is anyone with authority to make decisions on behalf of the patient, either a holder of a 'property and affairs' Lasting Power of Attorney10 or a deputy11 appointed by the Court of Protection. In practice the attorney or deputy will often be a relative or friend of the patient.

10.15.5 If an attorney or deputy is available, they must be consulted on what to do with the patient's property. They should be informed that the organisation will not accept liability for the patient's property unless it is handed over to the organisation for safekeeping. They should be

encouraged to remove from the premises any property (especially valuables) that the patient does not need, or otherwise to hand it over for safekeeping.

10.15.6 In cases where an attorney or deputy is not immediately available, staff may decide to take part or all of the patient's property into safe custody, if this is in the best interests of the patient. An attorney or deputy will however have to be involved in later decisions about the property. More details on attorneys and deputies, and on how staff should involve them in decisions, are provided in the Code of Practice.

10.15.7 Staff should bear in mind that even where a patient is assessed as lacking capacity to make a decision, they should be involved as fully as possible in the decision. For example, when deciding which of a patient's belongings to remove from their bedside, every effort should be made to consider their wishes and feelings in this regard.

10.15.8 The procedure for taking into safe custody the property of a patient who lacks capacity to decide is much the same as for deposited property generally. Where the patient is not attended by an attorney or deputy, two members of staff will need to place their signatures on the property book. The property will then be placed into safekeeping until the patient regains capacity to decide what should be done with it, or until the property can be given to the attorney or deputy. Where items are handed over for safekeeping by the attorney or deputy, their signature is required in the property book wherever it is required for the patient.

10.15.9 Where a patient is discharged and lacks capacity to make a decision about their property; any deposited property should be given to their attorney or deputy, obtaining their signature on the appropriate documentation.

11 UNCLAIMED PROPERTIES

11.1.1 Property that is unclaimed following patients' discharge, and of low value, may be disposed of as the Trust pleases. Care should be taken to ascertain whether articles are of value and hasty action to dispose of an article is unwise. Expert advice should be sought if there is any doubt about the value.

11.1.2 Unclaimed articles are valuable, every effort should be made to trace the owner or next of kin, but if this is not successful, articles should be kept for a reasonable time before disposal. Under the Limitation Act 1949, a period of six years would normally be reasonable.

11.1.3 The proceeds of the sale of unclaimed property should be credited to the exchequer account. If the property is inappropriate for sale, it should be destroyed. This should be recorded in the patient property record and signed by two members of staff, one being the cashier/PWO.

11.1.4 Any Bank/Building Society/Post Office books or National Savings Certificates should be returned to the issuing institution with an explanation of the circumstances that they came into the Trust's possession for safe keeping. They need to be signed out in the property record by two members of staff, one being the cashier/PWO

11.2 The Disposal of Unclaimed and lost property

The Portering Services Manager is responsible for dealing with the provisions under this section. Where an owner is known, reasonable efforts will be made to return the property by the Portering Services Manager.
Where, despite a reasonable effort being made to establish ownership and the owner is not known, Standing Financial Instructions will be followed. The property will be handled over to

the Trust's Supplies Department who will arrange for them to be sold and the proceeds credited to the Trust's Charitable Fund.

11.3. Children and Young Person

Children / Young Person will be encouraged to send any valuables home with their parent / guardian. If items of value remain on the ward the nurse responsible for care will liaise with the child/ young person or parent / guardian as appropriate regarding the completion of the attached form (See Appendix 2).

SECTION TWO

12 Key Safe Codes:

This section is mainly for community health services staff and any other staff that deals with patients using key safes.

12.1 What are key safes?

Key-safes are devices that can be fitted externally to a property to enable access into the property. In order to gain access, most key safes require a code that will release the cover and therefore allow access to the keys.
Key safes are used to enable safe entry to patients' houses by health professionals (and other agencies) where patients are unable to open the door themselves due to physical or mental impairment / illness or disability.

A key-safe is protected with combinations to hold keys of different kinds. These are mainly house keys but other keys, such as drug box or syringe driver keys, may also be stored there. They are available with manual dial combination input system or digital input system and are usually mounted on the wall in any space that is hidden or mostly unnoticed.
Some of the key-safes available in the market look like utility boxes, which makes them camouflaged/ covered and are often mounted near the meter box. Some, by necessity, are more obvious.

Community Health staff members are responsible for accessing patients' homes with their consent and permission, in order to provide care. Staff may be issued with codes for accessing key-safes in order to gain authorised entry into patients' homes.
The Health and Safety at Work Act 1974 places several duties on employers including the following:

"It shall be the duty of every employer to ensure, in so far as is reasonably practicable, the health, safety and welfare at work of all its employees."

(Section 2(1)) and "the provision and maintenance of plans and systems of work that are, so far as is reasonably practicable, safe and without risks to health." (Section 2(2a)) Therefore this policy hopes to provide protection for staff while handling patient's keys and security for patients while under East London NHS Foundation Trust Community Care Services.

12.2 Principles

- Key safes are to be accessed for the benefit of the service user and for the provision of care only.
- The property should only be accessed to carry out the care plan and for failed access.
- All Staff should be fully aware of their responsibilities regarding security and wellbeing of patients and themselves.

12.3 Responsibilities:

Everyone involved in patient care is responsible for ensuring that entry into and exit from patients' homes does not compromise their safety.

12.3.1 Staff Member:

Entry to patient's home

All Staff should:

- Ensure that their Skyguard device is on.
- Knock or ring doorbell before entering property, and wait for a reply.
- Introduce themselves and seek consent to access patient's home if necessary.
- Always show proof of identity / Trust ID card.
- Comply with patients' wishes especially where shoe protectors are required.
- Close doors firmly behind them.

12.3.2 Line Manager:

- The manager responsible for each team will designate members of staff to act as responsible key-safe code holders.
- Key-safe code holders will be responsible for the confidentiality of the key-safe code. and maintaining the security of the codes whilst in the community.
- The manager will act on behalf the Trust to ensure adequate records are kept and maintained according to local guidelines, If there is a security breach, the details must be recorded including what action was taken and by whom.

12.4 If Patient Is Unable To Open the Door Themselves

- Consider if a nearby relative or carer can act as key holder with patients' consent and enable access for healthcare staff.
- If no alternative method of access, assess for provision of a key safe and or refer to Social services for installation.

12.5 Key Safe Assessment

- Discuss with patient and family and obtain written consent for key safe.
- Document consent on EMIS /SYSTMONE, scan and upload consent form where appropriate.
- Consider who owns the property e.g. Housing Association, Residents Association and seek consent for installation of key safe.
- Assess size of key safe required e.g. standard or non-stock larger key safe.
- Consider location of key safe. Is there a suitable external wall that can be used? Is the type of wall suitable (brick or concrete)?
- Order and arrange fitting via TCES.
- If non stock key safe consider if Handyperson required to install and liaise with Social services or appropriate voluntary sector organisation for completion.

12.6 Key Safe – Safety & Security:

Please note that The National Back Office (NBO) Service Management team has received a number of incidents from concerned PDS (Personal Demographic Service) Users who have noticed that access codes for Key Safe boxes and other such door entry systems are being stored within the address field on the national patient index (PDS). The Head of Information Governance at the Department of Health has advised that this practise must cease immediately. The storage of these details on the PDS constitutes a security risk to vulnerable/elderly residents and in some cases the door entry codes have been printed as

part of the address on correspondence. These access codes must be stored securely at a local level and if they are stored electronically the data must not be synchronised with the PDS.

Therefore:

- Staff should take all reasonable steps to ensure that key codes are kept confidential.
- Key safe codes should not be shared with other individuals outside the team without the patients consent.
- As soon as key safe need is identified and agreed, inform the patient that other members of the wider team e.g. nurses, therapists, might use the key code to gain access as and when required.
- Record patient's key safe code on EMIS under *Initial Assessment / Social Assessment / Patient Door Access Key Code.*
- For System One Users, please record key safe code on *patients' home page under normal priority.*
- All keys should be secured appropriately in the key safe after use
- The key(s) must be returned to the key safe once the door has been opened, and the key safe securely closed, locked, with the codes 'jumbled' up each time it is used.
- When leaving the property ensure that the door is properly locked, using the key if necessary.

12.7 Mobile working:

- Key safe codes should be accessible electronically via mobile working devices and should not be written down e.g. in diaries.
- *Add patient's key safe code to 'reason' field of patient's Visit Schedule. This will enable key safe code to be visible during mobile working.*
- Key codes should *not* be recorded as a patient "alert" on EMIS as these are visible to all staff accessing the patient's health record.

13. Entering and Exiting a Patient's Property via a Key Safe:

- Staff accessing a patient's property via a key safe should be aware that they still are entering someone's home as a guest, and should be respectful and follow usual steps of working within professional Code of Ethics and Conduct and the Trust guidelines.
- Staff should always knock or ring the bell prior to entering a patient's home via key safe so as to alert the patient to a visitor arriving.
- Staff should always announce their presence on entering the patient's home and show their ID card at all times.
- Special care should be taken to avoid startling patients with hearing or sight impairments hence the importance of ringing doorbell before entering the house.
- Prior to leaving the property, staff should check that the key has been returned to the key safe and the key safe is securely closed / locked.

14. Patients' Keys

- As a general rule, it is the policy of the service **NOT** to hold keys for patients' homes.
- In exceptional circumstances (for example the patient is for End of life care or if there is no suitable location for a key safe) the service may hold a key until an alternative arrangement can be made.
- In this case, staff must take utmost care of the patients' keys and ensure that it is kept at an agreed and safe place in the base / office at all times.
- Under no circumstances should patients' keys be taken home by any staff member.

- Loss or theft of patients' keys must be reported immediately to the team lead and the patient and / or family must also be notified. This must be recorded on In phase as well.
- If ELFT staff are responsible for losing the patients' keys, then once recorded on In phase, arrangement need to be made in collaboration with the patient and his/her family to replace the lost keys.

15. What To Do When a Patient Alleges That a Staff Member Has Stolen His /Her Property:

- In all incidents where a staff member has been alleged to have stolen a patient's property, either cash or any valuable item belonging to the patient receiving care under the community services, this should be immediately escalated to the team leader who will:
- Investigate and Report the loss to the Clinical Lead and the Police via the Emergency services non –urgent number 9 101 without delay and no later than **by the end of the shift.**
- Obtain a CAD number from the Police.
- Ensure an **In phase is completed no later than by the end of the shift** and the CAD number is recorded on In phase.
- Inform the patient and ensure that EMIS record of the patient indicates the loss and confirm the actions taken.
- Seek consent to inform the next of kin or relatives of the loss and the actions taken.
- If they lack capacity, the clinician should make a best interest decision
- If out of hours, inform the On Call Manager of the loss and confirm that the appropriate actions have been taken.
- Inform Richard Harwin – The Trust Health, Safety, Security and Emergency Planning Manager with details of loss together with CAD number obtained from the police.
- All staff concerned with this incident must treat the allegation seriously, keep an open mind and make reference to and be guided by the steps in the table in Appendix 5.

The Staff member should not:

- Investigate or ask leading questions of the victim or staff.
- Make assumptions or offer alternative explanations.
- They must:
- Give assurance that information will be shared on need to know basis only.
- Make a written record of the information using the words supplied by the complainant.
- Ensure that all written records must be signed and dated and recorded on EMIS.
- If allegation involves children, the staff should inform their line manager and the Trust Safeguarding Lead, the relevant social care department and the police
- If allegations involves adult at risk of abuse or neglect, then speak with the patient if possible and ask him/her what happened and what remedy or outcome they want.
- Staff to speak with their line manager and the Trust Adult Safeguarding Lead, the relevant social care department and the police.
- Complete an IN PHASE of the incident.

Following an Allegation:

- The individual making the allegation should be offered or signposted to appropriate support, and his/her mental capacity established.
- Strategy Meeting /discussions between the GP, Community health services, police and social care must take place to confirm immediate and next steps.

- Investigation should include who was there when item went missing, what went missing, who else visits the patient, who was there prior to the staff members visit and what did they see etc.
- Unless the allegation is substantiated with evidence, the concerned staff member should continue to visit the patient, but accompanied by another colleague.
- During investigation, the patient should be visited by two staff members in the team, for protection of both parties.
- The CCG must be notified of serious incidents.
- Lessons learnt from this incident should be shared with the wider staff.

Support for Staff

- Employee Advice Programme via Occupational health should be offered to the staff through the Human Resources department.
- Following an allegation against a member of staff, he/she will be advised to contact their union or professional organisation as soon as possible for support.

The member of staff will be:

- Treated fairly and with dignity and helped to understand the concerns expressed and the processes involved.
- Be kept informed of the progress and outcome of any investigation and the implications for any disciplinary or related process; except where this could impede the investigation.
- Offered appropriate support through the Human Resources.
- If suspended, staff member will be kept up to date about events in the workplace and the Disciplinary policy will be followed if necessary.

15.1 Confidentiality

The Trust will maintain confidentiality and guard against publicity whilst an allegation is being investigated. Information will be restricted at all times to need to know basis in order to prevent fake news. The Trust will deal with enquiries, manage confidentiality and manage related disciplinary processes.

15.2 Investigating an Allegation

This may include:

- A police investigation of a possible criminal offence.
- Social Care enquiries or assessment about whether an adult at risk of abuse or neglect / child is in need of protection or services.
- Disciplinary action by the Trust

In all cases, appropriate Trust policy will be applied.

16. Monitoring and Audit

Standards	Monitoring and Audit			
	Method	**By**	**Frequency**	**Reviewed by and actions arising followed up by**
Appropriate storage and documentation of property at ward level.	Audit of property books	Ward Managers / Matrons	Quarterly	Nursing Development Steering group
Awareness and understanding of policy	Survey of all staff	Locality Leads	Annually	Report to Local Clinical Governance meeting
Key safe numbers documented safely on EMIS	Audit of key safe on clinical patients records	Team Leads	Twice a year	Assurance provided via the clinical lead at Clinical Governance meeting.

17. Policy review

This policy will be reviewed 4 years as a minimum unless for exceptionally business related reasons or any national or statutory changes dictate a need for an earlier review.

East London
NHS Foundation Trust

Appendix 1

DISCLAIMER NOTICE

Patients, relatives and visitors are encouraged to hand patients' valuable property including monies to staff for safekeeping.

THE TRUST CANNOT ACCEPT RESPONSIBILITY FOR THE LOSS OR DAMAGE TO VALUABLE PROPERTY AND MONIES NOT HANDED IN FOR SAFEKEEPING.

Appendix 2

PATIENTS' DISCLAIMER

Patient Name:

Ward / Department:

Date:

Please read the following before signing this form:

You have been informed of the Trust's arrangement for the safekeeping of Valuables. You have been advised to hand over your valuables for safekeeping whilst you are in hospital.

You have decided to take responsibility for all your valuables whilst you remain in hospital.

East London NHS Foundation Trust accepts **NO** responsibility for loss or damage to any of your valuables.

I have read and understood the above.

Patient / Representative:

Signature: …….

Print Name: ……. Date: ……

Witnessed by:

Staff Signatures: 1. ……... 2. …… **Date:** …….

Print Name: 1. ……2…… **Date**: ……...

Appendix 3

Managing patients money – simple guidance

DO'S	DON'T
Make sure that you are familiar with the Managing Patients Property Policy and local procedures.	Lending or giving money to a patient or buying items on their behalf is a serious breach and puts you at risk of possible disciplinary actions. There are many ways a patient can have access to funds – use only approved methods. Contact the Welfare Officer or Cashier for guidance or advice.
Discourage patients from retaining large sums of money.	Putting patient's money in a locked drawer, leaves it open to theft.
Help to make patients aware over how they may access their funds or buy personal items whilst in hospital	Do not act as proxy for the patients in making withdrawals.
Encourage patients' visitors to advise you if they have left money with a patient. You may need to encourage the patient to send the excess money to cashier.	Under no circumstances should staff make withdrawals or purchases on behalf of a patient using the patients' bank card. Patients should never be asked to disclose their PIN.

Appendix 4

Patient Welfare Officer (PWO) Procedures.

- The PWO has a key role to play in terms of the co-ordination of patients' property and financial affairs and as the key liaison point for relatives concerned with patients' property during a hospital stay or on death or discharge. In addition, the PWO has a role to play in terms of the appropriate disposal of the property of deceased patients.

- Because of this the PWO is placed in a vulnerable position and could face unreasonable allegations of misuse of patients' property. The procedure given below introduce a number of controls which if following with the PWO , should offer protection from such allegations, and also ensure that patients property is held, adequately recorded and appropriately disposed of on death or discharge.

RECORDING OF PATIENTS PROPERTY TRANSACTIONS

Individual Patient Property Balances

- The PWO is responsible for maintaining a system of individual patient property records. These should record all property held by the trust on behalf of each patient, their opening cash balance deposited with the Trust and any further deposits or withdrawals taking place during their hospital stay.

- When a patient is admitted to hospital, the PWO should receive a copy of the Patient's Property Record from the ward and this should be filed alphabetically in a centralised file. Based on this the PWO should then set up a new individual record on the computerised patient property system.

- The PWO should reconcile each patient balance on a monthly basis and the details of this and an aggregated summary should be forwarded to the finance department.

- The PWO should, through monitoring balances, ensure that patients' accounts do not go into arrears. If necessary the PWO should liaise with relatives or chase the Department of Work & Pensions (DWP) to make pension or other benefit payments.

- In exceptional circumstances, the PWO has the discretion to permit small amounts of expenditure (approx. £5 per day) to a patient with a nil balance, provided there is reasonable likelihood that income will be received in the future (i.e. from the DWP). If this is not the case, the PWO should bring the matter to the attention of the service management and the Deputy Director of Finance.

Pension and Benefits

- Patients admitted to hospital may be in receipt of benefits or pensions from the DWP. The Trust may act as an agent for patients who do not have relatives to attend to their financial affairs. On receipt of the admission copy of the PPR, the PWO should check the patient's pension and benefits status.

- If the patient wishes, the PWO can arrange for temporary payments from the DWP whilst they are in hospital. For long term patients, arrangements can be made for BACS payments into the Trust Bank account on the patients' behalf. The Financial Accountant will be responsible for notifying the PWO of any payments received by BACS on a weekly basis

- The PWO will deposit all Giros received with the Cashier for banking on the patients' behalf.

- The PWO should update the individual patient records on the Trojan computerised system when BACS payments are notified and when receipts are received from the Cashier in respect of Giro/cash/cheque deposits.

ORGANISING PATIENT PAYMENT OR REIMBURSEMENT REQUESTS

- The PWO is responsible for coordinating individual patient payment requests for utility and other domestic bills. The details should be summarised on a "Request for Payment from Patients Monies (RPPM)" form. One of these should be completed for each payee and the individual payment requests should be attached for audit purposes. Authorisation should then be obtained from the Service Manager, the Assistant Service Manager or the Acute Services Manager.

- The RPPM should then be forwarded to the Finance department who will make the appropriate payment. The PWO should update the individual patient property records accordingly.

- The PWO, if necessary, should advise the Cashier in relation to daily maximums for each patient, depending on their financial circumstances and with agreement of the senior clinical staff. Should there be any disagreement by the patient regarding this arrangement, the nurse in charge should countersign the withdrawal if it is approved. Should the clinical staff refuse the payment but there continues to be issues around this, it should be brought to the attention of the Deputy or Director of Finance, as we have a duty of care to our patients and to help prevent misuse/misappropriate of their funds whilst under our care.

Pension and Benefits Arrangements

- The PWO should write to the DWP enclosing a copy of the Certificate of Registration of Death advising them to cease paying pensions or other benefits. If payments are received after death, the PWO should ensure that these are included in the final balance payment to the next-of-kin or Treasury Solicitor.

MAINTAINING ACCURATE RECORDS

- To comply with the data protection act, you must ensure that all data held on the Trojan system is accurate and up to date. You should ensure that the current Rio number is held for each patient and if necessary, amend it from the old PAS numbers.
- If temporary numbers are used to set up a Trojan account for a patient, whilst awaiting registration, it should be a priority to convert this to a Rio number as soon as registration is complete – no longer than two days.
- No money should be held on the system for discharged patients. All efforts should be made to locate the discharged patient and return their monies/property to them. On the rare occasion that a discharged patient cannot be traced, email the Financial Accountant with an overview of the attempts made at finding the patient (Rio, Medical Records, writing to last known patient address/contacting next of kin), copies of any correspondence sent/received and the amount held on account by the patient. Confirmation by the Financial Accountant will subsequently be given that the individual patient record can be closed and archived by the PWO. These funds will remain available to the patient should they ever be re-admitted.

APPENDIX 5

RESPONSE TO ALLEGATION

Immediate response to allegation of stealing being made in patients' home	Management response to concern
• Complete Safeguarding referral and contact relevant social care department if appropriate. • Ensure adult is not at risk of abuse or neglect; safeguard child / children's immediate safety. • For protection of both parties, staff members to visit patients in company of another colleague. • If Safeguarding concerns are alleged, remove alleged perpetrator from patients contact immediately • Complete IN PHASE and record allegation documenting in line with Trust policy. • Inform line manager and Trust Safeguarding Lead immediately. If out of hours notify the manager on call • Do not investigate and question the patient / victim. • Do ask any relevant staff who may have witnessed incident to record what they have witnessed. Inform them that they must not discuss this incident with each other or any other staff member to ensure dignity and integrity of all involved is maintained • Contact police, ensure noted the crime reference number and police officer name and collar number • In conversation with police, agree any key points in relation to obtaining / preserving evidence. • Implement the Duty of Candour by informing patient's next of kin / relatives of incident and procedures to be followed, giving timelines and agreeing on how updates will be given.	Trust internal investigation should only move forward when agreed with police to ensure that no criminal investigation is prejudiced. • Ensure all actions in immediate response are completed and documented. • Ensure earliest liaison with Trust Safeguarding Lead and other leads connected to the investigation • HR manager will liaise with all concerned to undertake strategy discussions with, the Trust Safeguarding Lead / Senior Management in the Department of Nursing, other named professionals & communications throughout the process • Contact will be maintained with the concerned staff as per Trust HR policies and return to work of professional, or other action, will be agreed in strategy with relevant agencies / professionals / leads • The incident must be reported and investigated as a Serious Incident (SI) **Note potential outcomes:** • Possible Criminal Offence committed and court action • Demonstrable False Allegation • Significant Harm is demonstrated • Trust investigation and possible dismissal • Referral to appropriate professional regulatory body e.g. NMC, HCPC or GMC.