Lincolnshire Partnership
NHS Foundation Trust

REF: Policy 8a

Lincolnshire Partnership NHS Foundation Trust (LPFT)

Records Lifecycle Management and Information Governance Policy

DOCUMENT VERSION CONTROL	
Document Type and Title:	Policy
New or Replacing:	Replaced
Version No:	7.0
Date Policy First Written:	November 2011
Date Policy First Implemented:	1 August 2012
Date Policy Last Reviewed and Updated:	13 June 2018
Implementation Date:	2nd October 2018
Author:	Team Leader - Information Governance, Records and Privacy
Approving Body:	Information Management and Technology Committee
Approval Date:	1st October 2018
Committee, Group or Individual Monitoring the Document	Records Management and Information Governance Group
Review Date:	October 2019

RECORDS LIFECYCLE MANAGEMENT AND INFORMATION GOVERNANCE POLICY SUMMARY

Records of NHS organisations are public records in accordance with schedule 1 of the Public Records Act 1958 and its significant amendments which came into effect in 2005 and are up to date with all changes known to be in force on or before 12 June 2018. This includes records controlled by organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of their format. The Act requires all public bodies to have effective systems to deliver their functions. All NHS organisations have a duty under the Public Records Act 1958 to make arrangements for the safekeeping and eventual disposal of all types of records.

This policy relates to all clinical and non-clinical operational records and information held in any format by the Trust. This policy document pulls together the former arrangements covered by the policies for Freedom of Information, Records Management, Information Governance, Access to Health and Social Care Records, Scanning Paper Documents, Sharing letters with Service Users, Confidentiality and Data Protection, Data Standards, Provision of Information to Service Users and Carers and Clinical Coding and Data Quality.

Involvement in the redesign of the policy has been sought from membership of the current groups responsible for policy formation and monitoring. Those groups, as identified in the Duties table, will be responsible for the ongoing monitoring of the policy and ensuring that standards are measured and reported through to the Information Management and Technology Committee.

This policy is split into two sections. The first section sets the standards and legal requirements for policy implementation. The second section is a set of appendices which detail specific procedures for achievement of the policy standards.

Forms which support delivery of the policy have been hyperlinked so that they always connect to the master copy of the form in use by the Trust. For anyone accessing the policy outside the Trust, copies of forms can be requested from records@lpft.nhs.uk

This policy needs to be read in conjunction with both the Information Management and Technology Strategy and the Records Management and Information Lifecycle Strategy.

1. Records Management

Standards

1.1 Lincolnshire Partnership NHS Foundation Trust (the Trust) is required to deliver services to its service users ensuring that the healthcare records and information of the organisation are managed in accordance with the Data Protection Act 2018 which is the United Kingdom's implementation of the the General Data Protection Regulations (GDPR), Freedom of Information Act 2000, Records Management Code of Practice for Health and Social Care 2016, Confidentiality NHS Code of Practice 2003 and other professional bodies standards where applicable.

1.2 The Trust's records and Information are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support future operations and day to day delivery of high quality care for the purpose of accountability, and for an awareness and understanding of its history and procedures. Records and information supports policy formation and management decision making, protects the interests of the Trust and the rights of service users, staff, stakeholders and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.3 The Data Protection Act 2018 controls how personal information is used by organisations and organisations must make formal notification of their processing to the Information Commissioner and register as a Data Controller. The Trust is a Data Controller and must abide by the terms of its registration. This means that the Trust must also abide by data protection articles and principles so that personal information the Trust processes is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Everyone responsible for using personal data had to follow the rules of the above principles. This document should be interpreted in a way compatible with these principles and rights.

1.4 In order to comply with the relevant legislation, regulations, guidance and national standards as well as enhancing operational performance the Trust aims to ensure:

- **Records are available when needed** – from which the Trust is able to form a reconstruction of activities or events that have taken place;
- **Records can be accessed** – records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **Records can be interpreted** – the content of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;

- **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **Records can be maintained through time** - the qualities of; availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **Records are secure** – from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in robust format which remains readable for as long as required;
- **Records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff are trained** – so that all staff are made aware of their responsibilities for record keeping and records management.

1.5 The term lifecycle in the field of information refers to the lifespan of a record (paper or electronic) from creation to destruction, including information, acquisition, creation, retention, storage, retrieval, communication, utilisation and eventual destruction. Three main stages in the life of any record can be identified, regardless of how long each stage lasts. These stages can be viewed as follows:

STAGE 1 CREATION/RECEIPT	STAGE 2 MAINTENANCE	STAGE 3 DISPOSAL
The record is then either in frequent use or in regular current use so its importance, impact or administrative value remains consistently high.	Administrative value remains moderate. However records should be reviewed regularly and retained or removed according to their continued relevance or otherwise. Consideration should be given to the consignment of declining records to alternative store.	Maximum retention period is reached. The record ceases to have administrative value but should be considered for its possible historic value before being disposed of in an appropriate manner or sent for permanent archiving. Consult Team Leader - Information Governance, Records and Privacy

1.6 This policy will apply to all employees of the Trust, including Non-Executive Directors, Governors, bank staff, volunteers, individuals on secondment and trainees, or those on a training placement within the Trust and temporary staff employed through an agency. Staff from other organisations or companies undertaking work on Trust premises must abide by the relevant legislation and regulations and should be made aware of the pertinent parts of this policy.

1.7 If staff are unsure of their responsibilities at any time they should discuss this with their line manager. If managers are unsure of their responsibilities or the legal implications of their action the manager should contact the Records Management Team. In the first instance all requests for advice or assistance should be made by telephone/email

providing background information to the situation, the specific question being asked, the risks and the urgency of the request. Queries can be sent securely from outlook email accounts to records@lpft.nhs.uk.

1.8 Breaches of this policy will be taken very seriously and may result in disciplinary action.

1.9 The Trust has a duty to prepare for emergencies and to ensure that critical services can be delivered at an acceptable level and return to normal working practice as soon as the emergency situation has resolved. Information is classed as a critical service and therefore staff are reminded of the need to ensure that they refer to their area's business continuity plans for management of records in an emergency situation.

2. INFORMATION GOVERNANCE

2.1 Standards

As holders of patient information and systems the Trust is obliged to ensure that this information is held securely and handled correctly. The Trust submitted its Information Governance Statement of Compliance in 2007. Since then the Trust has had an annual requirement to provide evidence and assurance that they are practising good data security through the on-line Data Security and Protection Toolkit (DSPT). This is independently audited so that assurance can be provided to Trust Board level.

This on-line tool uses assertions to allow organisations to measure and evidence their performance against the National Data Guardian's 10 Data Security Standards. These standards come under three Trust Board Leadership Obligations:

Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Data Security Standard 2: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Information Governance has the following fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information to include the confidentiality, security, integrity and availability of patient, staff and business information
- To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way

The Trust supports the national agenda with the following work areas from the Information Governance Management Framework:-

- **Information Governance Management:**
    - Approved and comprehensive Information Governance (IG) policies and associated strategies and/or improvement plans that meet IG needs.
    - Formal contractual arrangements that incorporate the IG requirements are in place with all contractors and support organisations.
    - Employment contracts which include compliance with IG standards are in place for all individuals carrying out work on behalf of the organisation.
    - Awareness and mandatory annual IG training programmes for staff to ensure that all staff are suitably informed about their responsibilities.

- **Confidentiality and Data Protection Assurance:**

    - Adequate access to appropriately trained staff with suitable confidentiality and data protection skills, knowledge and experience.
    - Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users, and on the duty to share information for care purposes.
    - Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected.
    - Individuals are informed about the proposed uses of their personal information.
    - There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data.
    - There are appropriate confidentiality and audit procedures to monitor access to confidential personal information.
    - Protocols govern the routine sharing of personal information, agreed with other organisations.
    - All new processes, services, information systems and other relevant assets are developed and implemented in a secure and structured manner to comply with IG security accreditation, information quality and confidentiality and data protection requirements.
    - All person identifiable data processed outside of the UK complies with the Data Protection Act 2018 and Department of Health guidelines.

- **Information and Cyber Security Assurance:**

    - Adequate access to appropriately trained staff with suitable information security skills, knowledge and experience.
    - Appropriate management policies in place to direct the Trust's overall approach to cyber security.
    - A formal information risk assessment and information asset management programme for the appropriate management of key information assets.
    - There are documented information security incident / event reporting and management procedures that are accessible to all staff and that satisfy the Organisation's obligation as a Registration Authority.
    - Monitoring and enforcement processes are in place to ensure that NHS national application Smartcard users comply with the terms and conditions of use.
    - Operating and application information systems, under the Organisation's control, support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.
    - The Organisation's Senior Information Risk Owner (SIRO) takes ownership of the Organisation's information risk policy and information risk management strategy.
    - All transfers of hard copy and digital person identifiable and sensitive (or special category) information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers.
    - Business Continuity Plans are up-to-date and tested for all critical information assets (data processing facilities, communications services and data) and service-specific measures are in place.
    - Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error.
    - Information assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code.

- Policy and procedures are in place to ensure that Information Communication Technology (ICT) Networks operate securely.
- Policy and procedures ensure that mobile computing and tele-working are secure.
- All information assets that hold or are personal data, are protected by appropriate organisational and technical measures.
- The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate.

- **Clinical Information Assurance:**

  - The IG Agenda is supported by adequate information quality and records management skills, knowledge and experience.
  - There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements.
  - Procedures are in place to ensure the accuracy of service user information on all systems and/or records that support the provision of care.
  - A multi-professional audit of clinical records across all specialties has been undertaken.
  - Procedures are in place for monitoring the availability of paper healthcare records and tracing missing records.

- **Secondary Use Assurance:**

  - National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop.
  - External data quality reports are used for monitoring and improving data quality.
  - Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained.
  - There is a robust programme of internal and external data quality audit.

- **Corporate Information Assurance:**

  - Documented and implemented procedures are in place for the effective management of corporate records.
  - Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000.
  - As part of the information lifecycle management strategy, audits of corporate records are undertaken.

3. DATA QUALITY

3.1 Rationale

The recording of data in an accurate, complete and timely fashion will support Organisational, Management and Operational processes, decision making and statistical provision. Improving data quality and its completeness is an on-going process that changes regularly as a result of the demands services make for data and information.

Poor quality information can create clinical risk, cause inconvenience or worse to service users and staff, compromise effective decision making and impact on the Trust's ability to monitor standards of care and secure income for its services.

If information and data is valid, reliable, complete and timely then this implies:

- It is available to those who need it, when it is needed
- It is free from error
- It is formatted to satisfy organisational requirements
- It truly reflects the event or activity that it purports to
- There are proper management and security measures to protect it from unauthorised access

If data quality is weak this could provide an inaccurate picture of performance.

Accurate, up-to-date and accessible information (including appropriate clinical coding) is necessary for:

- Supporting the delivery of safe and effective care to service users
- Evidencing the rationale for clinical decision making/action
- Operational management and service improvement
- Demonstrating activity to Commissioners (and others such as NHS Improvement, Department of Health and the Public Expenditure Survey) and determining patient level income
- Evidencing achievement of targets
- Benchmarking
- Strategic planning and Board level decision making including need for new service provision
- Reporting to regulatory bodies (e.g. NHS Improvement, NHS Digital, NHS England, Commissioners and Care Quality Commission (CQC)) on performance
- Underpinning of Service Line Reporting
- Meaningful research and epidemiological studies

All staff have an obligation to ensure that all information they hold is valid, reliable, complete and recorded in a timely fashion.

Only as much information as is necessary should be gathered and recorded for the agreed purpose and avoid duplication.

All information collected and/or recorded during the course of the employment of all staff or individuals that work within or on behalf of the Trust remains the sole property of the Trust.

3.2 Standards

Organisations should ensure that the Completeness and Validity check for data as detailed in the guidance below has been completed and passed, with an average score of at least 6 achieved. (See Appendix 10)

3.2.1 Completeness and Validity Data Check

3.2.1.1. Introduction

1. All NHS organisations have a responsibility to ensure their data is accurate to comply with the *Data Protection Act 2018*, and fit for purpose, ready for migration to the national systems if appropriate. Each organisation should ensure that they establish a data quality leadership team which will lead on local plans to ensure good quality. These teams should be available to offer advice and guidance on a variety of data quality issues.
2. Staff should make a difference by ensuring, for example, that they include service users' NHS Numbers on all communications within the NHS and to service users themselves. Staff should where available also use the NHS Service Spine Portal – NHS Summary Care Record to trace and verify service users' demographic details and most importantly, their NHS Number. Access to the NHS Spine is controlled through smartcard authentication. Managers of staff wishing to access this service should request access is granted through the Team Leader Information Governance, Records and Privacy/Head of Informatics.
3. Organisations should also explain to service users why it is important that they identify themselves in a consistent way when they use NHS services - for example, asking a person called William, who is sometimes also known as Bill, to give the same form of his name each time and to ensure that the other names are captured.
4. The completeness and validity check for data must be completed and the average score calculated according to the national guidance.
5. Full details of data definitions and format specifications are referenced The NHS Data Model and Dictionary provides a reference point for approved Information Standards Notices to support health care activities within the NHS in England. It has been developed for everyone who is actively involved in the collection of data and the management of information in the NHS. The NHS Data Model and Dictionary is maintained and published by the NHS Data Model and Dictionary Service and all changes are governed by the Data Coordination Board (DCB) process. Changes are published as Information Standards Notices (ISN) and Data Dictionary Change Notices (DDCN).
6. The purpose of the analysis is for The Trust to be able to assure itself of the quality of the information produced. Completeness and Validity checks are simply one aspect of this.
7. The Trust is required to do analysis for each key data item.

3.2.1.2. Data Output Quality Standards

8. The performance standards for Completeness and Validity for each data group are:

- Required Standard to achieve **Attainment Level 1**
- Average score for completeness and validity, across all data items, greater than or equal to **two**
- Required Standard to achieve **Attainment Level 2**
- Average score for completeness and validity, across all data items, greater than or equal to **six**
- Required Standard to achieve **Attainment Level 3**
- Average score for completeness and validity, across all data items, greater than or equal to **Nine**

9. There needs to be an adjustment made for any duplicate records and that concerns over the completeness and validity of central returns will also lead to an adjustment of this score.

3.2.1.3. Data Quality in relation to Healthcare Records Management

All service users referred to the Trust will have an electronic healthcare record created, infrequently a subsidiary paper record may be created but this generally only applies to inpatient episodes of care. The systems in use by the Trust – RiO, Mosaic and IAPTus all have the functionality to hold practitioner records or also known as clinical notes.

All staff will resolve any issues identified with data quality for which they are accountable and will escalate any other data quality issues observed to the Records Management Team in the first instance by e-mail to records@lpft.nhs.uk The Records Management Team will review the situation and offer advice to rectify the situation and where necessary advise the service to raise an incident report should the severity of the issue warrant it.

All staff will keep up-to-date with any developments to the Electronic patient records to which they have access and attend any refresher training as necessary.

Access to Electronic patient records is available through the Informatics Team and staff will only gain access to the parts of the system which they require to undertake their specific role for the Trust. Access is undertaken in accordance with Role Based Access Controls to maintain confidentiality and appropriate access to information. Access will only be granted following completion of the access forms signed off by their manager and following systems training through the informatics team. When staff move locations/teams or leave the organisation the access forms must again be completed by managers to ensure that access is amended or removed as appropriate and further training as necessary is provided. Consideration should also be given to any corporate systems being used which may require access modification i.e. SHARON, ESR, Datix, E-Expenses, E-Series.

All discharges and transfers of patients from inpatient settings will be appropriately clinically coded. (See Appendix 9)

Where there is no entry in a health record for a significant period of time the next entry into the record should state clearly the reason for the break in recording of information.

When recording multi-disciplinary team (MDT) meetings or ward rounds into the healthcare running record it is essential that the names and designations of all those present at the event are documented in the entry made. It is also essential that the senior healthcare professional present is responsible for decision making and the time is noted. Admission, handovers, MDT's, Ward Rounds and discharges should all be recorded on standardised templates into the electronic record to ensure consistency of information recorded and to ensure that there are no gaps in delivery of care.

Should the service user's care delivery change between Consultants it is essential that the name of the new consultant responsible is documented by completing a transfer of care form and update the change on the appropriate electronic patient record.

All patient information systems have standards which must be complied with when entering data onto the system to ensure that data entered meets National data set standards. The standards required for RiO, Mosaic and IAPTus, are available by following this link.

3.3 Procedures

3.3.1 General Points

All documentation (entries in healthcare records, form completion, file notes, letters, emails, faxes etc.) should:

- Be accurate, complete and timely
- Be an accurate reflection of the event/action/care given
- Be free from the use of jargon and abbreviations
- Be legible
- Be in indelible black ink (if handwritten)
- Contain the date and time (24 hr clock) of the event/action/care given as well as the date and time the record was made.
- Be signed (this might be with an electronic signature i.e. email or through the system's own electronic audit trail) showing the author's designation.
- Every page of the healthcare record should clearly show the service user's NHS number.
- All letters are expected to be typed and sent on Trust letterhead paper to provide authenticity, maintain professionalism and promote legibility. The Trust letterhead template should be used available here.

NHS England has directed that NHS patient records will be paper free by 2020. To support achievement of this the Trust determined that with effect from 1 October 2014 the electronic patient record will be maintained as the "primary" source of clinical information.

Where historical records exist for patients in paper format they should be held for reference purposes only with the exception of the following paper forms

- Mental Health Act Section Forms
- Medication Cards

All other paper, correspondence, reports, assessments etc. will be scanned and attached to the relevant clinical system and the original paper document can be destroyed following a quality check to ensure that it is attached to the correct patient record and legible. The document centre scanning and filing is available for guidance on where to attach and also (see Appendix 13).

Our dependency on paper records must diminish in preparation for 2020; this enables us to reduce costs and risks and to ensure that our electronic records become a trusted source of information. There should be no need to print letters for storing in paper records or for review at appointments. Everything that the clinician requires to review is available on the relevant clinical system as the primary source of information.

Specific procedures can be seen in relation to records creation and maintenance (at Appendices 1 to 8).

4. INFORMATION SHARING AND ACCESS TO INFORMATION

4.1 Rationale

All employees of the Trust are responsible for maintaining confidentiality. The duty of confidentiality is written into employment contracts. Breach of confidentiality of information gained either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal. That duty of confidentiality continues even after employment has ended.

Computer Networks and Electronic patient records allow for the sharing of data easily. This can be essential to business activity. However, the method and degree of information sharing is governed by the 'need to know' Caldicott principle and compliance with statutory obligations, such as the Data Protection Act 2018 and the Confidentiality NHS Code of Practice.

Authorisation processes for each electronic system mean that appropriate recording and storage of information will lead to only those with the appropriate authorisation having access to the information.

As a consequence of an individual's employment by the Trust, they may acquire, or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by an authorised person on behalf of the Trust.

Where access is required to another individual's stored information for necessary business continuity purposes only the Chief Executive or an Executive Director can authorise IT to access or to grant access ensuring compliance with the Regulation of Investigatory Powers Act 2000 and individual's Human Rights. In this situation please refer to the ICT Systems Use Policy 8C for the form to be completed.

Although it is neither practicable nor necessary to seek an individual's specific consent each time information needs to be passed on for a particular purpose, for example health care, this is contingent on individuals having been fully informed of the purposes to which information about them may be used. This is done in accordance with Appendix 1. Should it become necessary to share information with agencies other than those originally notified to the service user, or to share information for other purposes than originally agreed, then the consent of the service user will usually need to be obtained.

Where service user information is extracted for other agreed purposes (for example audit) there must be a sound rationale for every piece of information that is used. Personal identifiers should be removed from the data for the intended use.

Public authorities have a statutory duty to comply with the Freedom of Information Act 2000. This gives members of the public the right to access non-confidential information held by the Trust, unless a detailed exemption applies. (See Appendix 22)

Requests for information from external sources can therefore be categorised in 4 ways: (1) data subject access request for confidential PID (where the individual is requesting sight of their record/or a copy – it might be healthcare record or personnel record. Also bear in mind that subject access requests can also come from appropriately authorised representatives); (2) third party access request for confidential PID; (3) requests for access to healthcare records from new healthcare providers (transfers of care) or (4) a Freedom of Information request for non-confidential information. Staff should identify what type. See Appendices 14 - 22 for procedures to follow.

The Trust is a signatory to the Lincolnshire Inter-Agency Information Sharing Protocol 8d on the policies pages of the Intranet. The Trust has documented Memoranda of Understanding with all partner agencies to underpin the routine sharing of information to better support cohesive service user care.

Where the request for access to information is from a new healthcare provider the former LPFT service delivering care should ensure that appropriate consent is sought from the service user, or a decision taken to share without their consent using best interest principles or the 7th Caldicott Principle. The documentation and process to be followed are contained in the Clinical Care Policy (Policy 1).

The NHS Plan 2000 required that "letters between clinicians about an individual service user's care will be copied to the service user as of right" (see Appendix 21 for specific procedure).

The advantages of copying letters to service users include:

- **More trust between service users and professionals: better informed service users:** Service users and carers have a better understanding of their condition and how they can help themselves
- **Better decisions:** Service users are more informed and better able to make decisions about treatment options
- **Better compliance:** Service users who understand the reasons for taking medication or treatment are more likely to follow advice
- **More accurate records:** Errors can be spotted and corrected by the service user
- **Better consultations:** Professionals can confirm that service users understand what is being said during the consultation. Service users are better prepared and less anxious
- **Health promotion:** The letters can be used to reinforce advice on self-care and life styles.
- **Clearer letters between professionals:** Letters written between professionals are clear and understandable to both professionals and service users and carers.

For service users receiving care but not on Care Programme Approach (CPA) their care of treatment plan may be contained within a letter. Specific guidance on CPA, care planning and associated documentation is contained in the Clinical Care Policy (see link above).

4.2 Standards

All staff will receive and sign for a copy of the Security and Confidentiality of patient and personal information Code of conduct for staff on start of employment through their mandatory attendance at induction.

Staff and service users must understand how we will use information about them. Achieving this understanding will therefore depend on giving the service user relevant details about the purposes of processing information and any likely disclosures. The practitioner responsible for the care of the service user must discuss the uses of their information with them and provide them with a copy of the How we use and share your information to help you, the leaflet is available in a number of different languages. The leaflet is useful as reinforcement of the information provided verbally but is not in itself sufficient. Any explanation should include as a minimum:

- The main use of the information will be to manage the service user's care and treatment and that it is very important that we have full and accurate information if we are to provide the best care.
- Personal information should only be used for the purpose for which it was obtained.
- That we also use their information to check the quality of the care that they and other service users receive, to ensure that this is of the right standard. This process is called audit. Everyone involved in audit has to follow the same strict rules on confidentiality.
- That you work as part of a team and will share information about the service user with the team if it is necessary to provide the best care for them. Explain who is a member of your team. If you work with members of another agency then you should explain that information may be passed to that agency if it is necessary to provide their care, but that the agency has also signed up to the same standards of confidentiality.
- That they have a right of access to their health records which can be explained on request and guidance followed at Appendix 17.
- That we send anonymous information to NHS Digital to allow us to manage the service and monitor its effectiveness.

It may also be appropriate or necessary to discuss the use of the subject's information at other times during their care, for example:

- When transferring their care to someone or somewhere else
- When their legal status changes (for example the section of the Mental Health Act 1983 which applies to them, or if they are diagnosed with a notifiable disease)

It is not usual practice to obtain written consent to the use of information for care or treatment although this is required for some other purposes such as research. If service users do not wish to have their information used for research purposes then they should notify the records team at records@lpft.nhs.uk and this will be documented on their electronic patient record.

The Trust now invites service users to sign a confidentiality and consent form which explains how we manage their information and who we are likely to share information with. It also informs them of their right to receive copies of letters written about them and they can express if they wish to have information routinely shared with any members of their personal care network i.e. family, friends, carers. It further covers the accessible information standard which details how they may wish to receive information if they have a communication needs relating to a disability or sensory loss. This might be requiring information in large print, audio, braille, easy read or maybe in an alternative language.

The Trust has publicised an Information Charter on the Trust's website which informs service users about the promise the Trust has made to protect their confidential information and the part service users need to play in ensuring that information held is accurate and up to date.

It is strictly forbidden for staff to search and view any information relating to themselves, their own family, friends or acquaintances unless they are legitimately involved in the service user's LPFT clinical care or legitimately involved with the employees administration on behalf of the Trust. If a member of your family or a friend for instance is receiving services from the team you work for, ensure that this is recorded with your manager in supervision and appropriate protection measures are put in place. Routine audits of access to information are undertaken by the Informatics team to protect the information held in clinical systems. Unauthorised access to confidential information will be viewed as a serious breach of confidentiality and will result in disciplinary action. Any allegations of inappropriate access will be subject to the Trust's protocol on systems access investigations which is Appendix C within the ICT Systems Use Policy 8C .

5. PROVISION OF INFORMATION TO SERVICE USERS AND CARERS (LEAFLETS)

5.1 Rationale

There is a need to provide our service users and their carers' with information in order for them to have the opportunity to make informed decisions and to improve understanding of the care they receive from the Trust. They are entitled to receive this information in a manner which is most appropriate to their needs whether that be a disability or language barrier which is detailed in the Accessible Information Standard.

The aim of this policy is to ensure that useful, relevant and timely information is available to service users and their carers', across all the services provided by the Trust. Information can come in a variety of formats, such as:

- **Written** – leaflets, fact sheets and posters
- **Electronic** – content on our website/intranet, downloadable documents
- **Audio/Visual** – sound clips, video footage, DVDs

The NHS Litigation Authority now NHS Resolution have identified the importance of having an effective process for developing, monitoring and archiving service user information associated with care, treatments and procedures.

The information in this policy relates specifically to information leaflets but should be referred to as good practice guidance when considering the need, production and implementation of other formats of information.

5.2 Standards

The purpose of this policy is to inform staff of the processes involved in requesting, producing and using information for service users. It also aims to encourage staff to consider the information their unit / team / service provides to service users by providing best practice guidance.

Good information is important, as it can:

- Give service users confidence so their overall experience as a service user is improved;
- Remind service users what they were told by their doctor, nurse, social worker or other Trust contact and provide it in a medium that is most accessible for them to understand;
- Allow people to make informed decisions, written information can be taken away giving them time to read the information and think about the issues involved;
- Involve service users and carers in their treatment and Trust services;
- Provide information to the public and promote Trust services.

The essential content of any Trust produced leaflet will be incorporated into a house-style template and as a minimum will include the following:

- Title
- Introduction and purpose of leaflet
- Main text to include risks, benefits and alternatives, if appropriate
- Conclusion
- Contacts for additional information

When producing information it is helpful to consider key points and questions to ensure the information available to service users is as comprehensive as possible. See How do I produce a service leaflet on the Trust's intranet. Authors should discuss leaflet content with the Communications Team. (See Appendix 25)

6. ARCHIVING, DESTRUCTION OR DISPOSAL OF INFORMATION

6.1 Rationale

The Trust maintains a locally adapted retention schedule (See Appendix 30) which is based on the national standards publicised in the Records Management Code of Practice for Health and Social Care 2016.

6.2 Standards

The Records Management Code of Practice for Health and Social Care 2016 gives clear instructions on the length of time records must be retained by the organisation and the requirement to destroy records after the prescribed length of time. There are some records that must not be destroyed and this process gives some examples of the reasons for non-destruction and the means by which such records should be identified. The Trust places records for permanent preservation in the approved place of deposit at Lincolnshire Archives.

The Trust has a large amount of records to maintain both current and archived. This requires the records to be managed efficiently to allow appropriate access to practitioners and service users and to ensure that records are destroyed safely and securely when their destruction date is reached.

A record of the destruction of records, showing their reference, description and date of destruction is maintained and preserved so the Trust has documented what records are no longer available. If contractors are used, they are required to sign a confidentiality undertaking and to produce written certification as proof of destruction and this is also maintained centrally by the Senior Records Management Advisor.

If staff require further information they should consult the full document or discuss with the Senior Records Management Advisor.

(See Appendices 6, 7, 23 and 30)

7. AUDIT OF INFORMATION

7.1 Rationale

The Records Management Code of Practice for Health and Social Care 2016 has been published by the Information Governance Alliance as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England.

The Trust healthcare records annual audit programme has been designed to enable the Trust to meet NHS standards and also its obligations in respect of the Data Security and Protection Toolkit (DSPT).

- Develop guidance on good practice with the aim of establishing common and consistent standards of record creation and record keeping within the Trust, taking into account current Data Protection and Freedom of Information legislation.

- To create and keep records which are adequate, consistent, and necessary for statutory, legal and business requirements.

- Identify all records vital to the continuing functioning of the activities of the Trust in the event of disaster and make provision for their protection (to be cross-referenced with the Trust Risk Management Strategy).

- Undertake an inventory of all Trust records, both health and corporate records held in either hard copy or electronic formats. (This is to ensure that all record collections/information sets are identified along with the volume of records held, the type of media on which they are held, their physical condition, their location, the environmental conditions in which they are stored and the responsible manager).

The Trust carries out an annual audit of clinical coding, based on national standards, undertaken by a Clinical Classifications Service (CCS) approved auditor.

7.2 Standards

Healthcare organisations have a responsibility to ensure that standards outlined by the Care Quality Commission, all NHS Bodies and Data Security and Protection Toolkit as a minimum are implemented and measured against to ensure delivery of high quality care and treatment. Achievement of this requires organisations to continually assess and measure performance of the Trust against standards required and set improvement action plans where delivery falls below the desired mark.

Audit is one means of undertaking this process and all audit activity is documented in the Trust's annual audit programme. Services are required to participate in audit in accordance with the annual plan and to utilise the approved audit tools agreed by the Trust. Action plans will be completed following audit and improvements monitored, measured and reported to the appropriate monitoring committees of the Board.

(See Appendix 24)

8. LEGISLATION, GUIDANCE AND POLICY

This policy is not a substitute for the legislation, regulations and Codes of Practice to which all staff must adhere. The list below is not intended to provide a complete list of the legislation governing the practice of NHS employees.

- Data Protection Act 2018 including European General Data Protection Regulations
- Human Rights Act 1998
- Mental Health Act 1983 revised 2007
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Freedom of Information Act 2000
- Health and Social Care (Quality and Safety) Act 2015
- Public Records Act 1958
- Copyright Design and Patents Act 1988
- Health and Safety at Work Act 1974
- Electronic Communications Act 2000
- Re-Use of Public Sector Information Regulations 2015
- NHS Care Records Guarantee for England
- Social Care Records Guarantee for England
- Accessible Information Standard
- Data Security and Protection Toolkit
- The NHS Confidentiality Code of Practice 2003 and Supplementary Guidance: Public Interest Disclosures 2010
- Information Security Management: NHS Code of Practice 2007
- Records Management Code of Practice for Health & Social Care 2016
- Caldicott Report 1997 and Caldicott "2" 2013
- Care Quality Commission and National Data Guardian review 2016
- Caldicott "3" Report 3 Leadership Obligations & 10 Data Security Standards
- Care Quality Commission Report Safe Data, Safe Care
- Department of Health Copying Letters to Patients Guidance 2003
- NHS England Safer Hospitals Safer Wards 2013
- A Guide to Confidentiality in Health and Social Care 2013
- Checklist Reporting and Managing Information Governance and Cyber Security Incidents 29 May 2015
- British Standard for Legal Admissibility and Evidential Weight of Information Stored Electronically (BSI BIP0008)
- DoH Copying Letters to Patients' Guidance 2003
- Regulation of Investigatory Powers Act 2016
- Electronic Communications Act 2000 and all applicable laws and regulations relating to Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

8.2 This policy has been written in consideration of the Care Quality Commission Regulations for Service Providers and Managers which relate to key Acts and regulations.

9. POLICY CONTROL INCLUDING ARCHIVING ARRANGEMENTS

This policy, the procedures and the associated documentation have been approved by the Information Management and Technology Committee and ratified by the Board of Directors. They will be reviewed by the IM&T Committee annually or sooner if required by changes to legislation or guidance. The Trust Secretary will maintain a version of old policies for the lifetime of the organisation in line with the recommendations contained within the Records Management Code of Practice for Health & Social Care 2016.

10. DISSEMINATION AND IMPLEMENTATION OF THE POLICY

This policy will be available through the Trust intranet linking to the Trust website as part of the Trust's information publication scheme process.

The policy will be implemented by making all staff aware of the contents of the policy through the Trust Intranet, the weekly word and other communications initiatives due to the high impact that this policy has on all those staff working within the organisation.

The groups with responsibility for the monitoring of the policy also have a requirement to include the policy provisions in routine meetings to ensure that service nominated representatives take information back to their respective teams across the Trust to ensure that all staff are made aware of the possible impact of implementation.

The provisions of the policy will be included in both induction training and mandatory training to make staff aware of their individual responsibilities and highlight risks associated with non-compliance both for the organisation and the individual.

All associated leaflets, forms and publications are available on the Trust website, intranet or through the print management contract as appropriate and will be continually reviewed and refreshed to ensure that they continue to meet the needs of the organisation and the service users for whom services are provided.

Appendix 1

Creation of Clinical Records on Referral Received and First Contact/Admission Process

The Service, in receipt of the referral, checks all available electronic patient record systems to see if the service user has previously accessed the Trust's service. Duplicate records pose a risk and therefore a minimum combination of three check should be performed using different source information (e.g. Name, DOB and NHS number etc).

Contact should also be made with the relevant records library to retrieve historical paper records for reference purposes.

On referral ensure the following information is received and recorded on the system:

GP checked and amended if necessary
NHS number
Referral to
Correct Clinical Unit
Source of Referral
Patient Address checked and amended if appropriate
Date and time referral received
Correct Directorate
Correct Care Option
Referrer Name and Address
Date of birth

Use NHS Spine to check most up to date demographics
This should be done within 3 days of receipt of referral or immediately on admission to a ward.

On referral ensure the following information is received and recorded on the system:

GP checked and amended if necessary
NHS number
Referral to
Correct Clinical Unit
Source of Referral
Patient address checked and amended if appropriate
Date and time referral received
Correct Directorate
Correct Care Option
Referrer Name and Address
Date of birth

Where necessary use NHS Spine to check the most up to date demographics
This should be done within 3 days of receipt of referral or immediately on admission to a ward.

At first contact/admission:

Verify identity of the service user*
Gender
Record Accommodation type and status
Record marital status
Main Language
Record religion
Nationality and immigration status
Other Names if appropriate (e.g. nick names, previous names, aliases)
Smoking status
Record Accessible Information Standards
Record Housing Status
Record Employment Status
Record details of children resident in the accommodation
Record ethnic group
Record next of kin and carer details or any other associated persons
Veteran Armed Forces status

Contact had by any staff member with a service user. The staff member should ensure that the service user understands how their information may be used and they are asked to complete the confidentiality and consent form, they have been provided with How we use and share your information to help you leaflet and they have been asked to clarify any relatives or carers with whom information can be shared as part of ongoing care

If the service user is not resident in the European Economic Area then the admission to an inpatient bed or emergency community treatment will need to be notified to the Finance Department at Trust HQ so that the relevant medical insurance can be ascertained and charges for treatment can be levied.

Check for existing open referral to care before creating a new one.
Appropriate and accurate dates must be recorded – referral date, contact dates, end care option date
Staff details recorded on the 'care network'
Check and record CPA classification if appropriate

Regularly review demographic details (including GP) with service user and ensure any relevant changes are made on the system. Refer to NHS Spine for most up to date information.

Regularly review caseloads and end the care option of any service users who are no longer receiving care from you.

It is expected that service users will only have paper notes to house certain information which needs to be retained in physical format i.e. Mental Health Act section papers and legal documents, medication cards (inpatient admissions only). Therefore on receipt of a new referral the service should ascertain if there is any requirement to create a physical paper healthcare record.

If duplicate electronic records are discovered the Informatics Team must be informed by logging a call to the IT Helpdesk and on the Datix Incident Reporting System. If duplicate historical paper healthcare records are discovered the Senior Records Management Advisor must be informed and both (or multiple) sets of records should be sent to the appropriate medical records library for merging.

Appendix 2

Recording Clinical Contacts and Events

All entries into the electronic healthcare record must be made within 24 hours of contact with a service user. Where, in exceptional circumstances, this is not practicable the entry should be made on the next working day. If you know that you will be unable to enter into the electronic patient record within 24 hours then rough notes must be made of the intervention. When the later entry is then made into the record it should be documented "written from notes made at the time" and it should state why the entry is being made late.

Ensure when the entry is made that the actual time of the event is clearly shown on the system, the system automatically documents the time the entry is being written to evidence that this is a retrospective entry into the notes.

Only Trust approved abbreviations are to be used when making entries into healthcare records.

Countersigning of records

Where a registered practitioner delegates the task of record keeping to a non-registered practitioner, the registered practitioner remains responsible for the task being completed to the required Trust policy standard.

Where, the delegated task is recording a contact or activity within a patient record, the registered practitioner remains responsible for:

- Ensuring the task delegated is within the competence of the non-registered practitioner;
- Ensuring the record keeping meets the required Trust policy standard.

In terms of appropriate delegation, guidance in the Nursing and Midwifery Council The Code (2015) under the 'Practice effectively section and more specifically within section 11 of The Code specifies:

As a Registered Nurse you are accountable for your decisions to delegate tasks and duties to other people. To achieve this, you must:

- only delegate tasks and duties that are within the other person's scope of competence, making sure that they fully understand your instructions
- make sure that everyone you delegate tasks to is adequately supervised and supported so they can provide safe and compassionate care, and
- confirm that the outcome of any task you have delegated to someone else meets the required standard.

If a registered nurse is satisfied the above criteria are met, then delegation of the record keeping activity will be appropriate and there will be no requirement for the registered nurse to countersign the notes.

Conversely, if there is any doubt about the individual's competence, then supervision and countersignatures will be required until they have received the appropriate level of training and are deemed competent to complete the activity.

In any event, a registered nurse should not be countersigning notes unless they have witnessed

or can validate the activity as having taken place.

The act of record keeping attracts the same principles as any other delegated task in the health and care setting, including the need for ongoing supervision as appropriate.

The registered nurse retains professional accountability for the appropriateness of the delegation of the task, but the HCA/AP/student takes on personal accountability for the content and quality of the records, in line with NMC guidance and organisational policy.

The NMC have produced a booklet called Delegating Record Keeping and Countersigning Records June 2017 from NMC Record Keeping

For patients on an inpatient ward there must be an entry made into the clinical notes for each shift of staff during the day to ensure that information is maintained in an accurate and reliable way and the views of staff on the health and presentation of the patient are continuously documented. The entry should clearly identify how the care plan is being delivered and any risks.

Should you discover that an erroneous entry has been made onto the electronic patient record system (i.e. clinical note attached to the wrong service user record or attachment into the wrong section of the file or on the wrong service user file) then the Informatics Team must be informed, as soon as possible, by logging a call to the IT helpdesk. This enables the Informatics Team to move the entry to the correct service user record. Use the system number to identify the service user to maintain confidentiality.

If the incorrect note is more than 24 hours old it should be recorded on the Datix incident management system as this error may impact on patient safety. This will provide an audit trial for the information that has been moved.

If the error has led to a breach of confidentiality this must be recorded on the Datix incident management system and your line manage must be informed.

All documents received or created in respect of the treatment of the service user must be scanned and attached to the electronic patient record. This ensures that information is available to teams wherever and whenever it is needed.

If documentation is scanned onto the wrong electronic patient record the incident must be completed on the Datix incident management system and noted in the electronic patient record and inform your line manager.

If the scanning error has led to an electronic patient record being created the Informatics Team must be informed by logging a call to the IT helpdesk. This enables the Informatics Team to move the documentation to the correct service user record. If the scanning error is more than 24 hours old it should be recorded on the Datix incident management system as this error may impact on patient safety. This will provide an audit trial for the information that has been moved.

If the error has led to a breach of confidentiality this must be recorded on the Datix incident management system and your line manage must be informed.

All contacts, interventions, liaison and work undertaken with the service user and their support network must be recorded on the electronic patient record. **All staff** (including medical staff) will make entries onto the clinical noting section of the system; there is no longer a provision for handwritten entries unless for business continuity purposes.

Where the service user has been seen for a review or assessment appointment it is expected that the subsequent correspondence will be sent within 7 working days. The service user should receive a copy of the correspondence which should only be amended if there are clinical grounds for doing so. A signed copy of all versions of the letter should be placed on the electronic patient record. Where medical staff rely on their correspondence to detail the content of their intervention with the patient they must create a clinical note to identify any immediate risks, medication or MHA changes and direct staff to the creation of the letter in the document centre.

Notified changes to a service user details/circumstances/death must be processed on the electronic patient record system within 24 hours. Where there is a service user death this should be notified to the Informatics Team by logging a call to the IT helpdesk and a clinical note added to the system to advise details of the death. Where the service user has been receiving services in the 6 months prior to their death this should be recorded on the Datix incident management system to enable the circumstances of their passing to be reviewed to determine if an investigation is required.

Adopted persons' electronic patient record can only be entered under a new name when an adoption order has been issued; before this an alias may be used but more commonly the birth names are used. Depending upon the circumstances of the adoption there may be a need to protect from disclosure any information about any third party. The patient should be directed to their GP to amend their GP records with the new name details and this will link through to their NHS number. If documentation is provided this can be scanned into the system under confidential information and the original paperwork returned to the service user. LPFT staff will then be able to update the Trust's electronic patient record systems with the information which will then successfully link to the NHS number.

Transgender persons' can have their gender changed in their record. The patient should be directed to their GP to amend their GP records with the new name details and this will link through to their NHS number. If documentation is provided this can be scanned into the system under confidential information and the original paperwork returned to the service user. LPFT staff will then be able to update the Trust's electronic patient record systems with the information which will then successfully link to the NHS number.

Staff are reminded that the use of paper diaries for management of clinical working commitments carries with it a risk to the information contained in the diary and therefore staff are urged to follow these basic principles.

- Consider if a paper diary is necessary or whether a smartphone or other encrypted portable device can be used to manage your daily activity whilst on the move.
- If a paper diary is essential then only the minimum person identifiable data should be recorded i.e. set of initials and perhaps a postcode to remind you of the location

If a paper diary contains information which can be used to identify a person i.e. patient names and addresses then it is classed the same as multiple sets of medical records and must be transported according to the process at Appendix 8. Any loss of this diary would be classed as a serious breach of confidentiality and would result in a serious investigation, therefore staff are advised to reconsider these working practices and adopt methods which are more robust.

Appendix 3

Corporate Information/Records – Creation, Use and Storage

Corporate information and records relates to all information held or created by the Trust that is anything other than a patient's healthcare record or staff member's personal HR record. The information may either be held in paper format or electronically. This therefore relates to areas of the Trust such as; Finance, Information, Human Resources, Payroll, Trust Board, Estates, Complaints, Legal or any other administrative process conducted anywhere within the Trust. It is important to maintain accurate records as they form the basis of our corporate memory; our past, present and future. This information is required to be maintained in accordance with statutory requirements and may also be subject to Freedom of Information Act requests.

All records must be completed legibly, accurately and appropriately. Meeting administrators should use the approved Agenda Template and Minutes Template available on SHARON in the templates folder under Communications and then select LPFT templates.

All documents should be marked appropriately to reflect the sensitivity of the corporate document.

OFFICIAL - SENSITIVE COMMERCIAL for use with Trust Board papers, contracts and tenders, commercial, not yet published information, proceedings not yet published, investigations, OFFICIAL – SENSITIVE PERSONAL for use with patient information, staff information, matters of personal nature between sender and recipient

Watermarking electronic documents ensures a document is labelled correctly for all to see. Staff should therefore use the following watermarks where this is appropriate: DRAFT – Any document, but especially policies or other documents for review and consultation should be marked "Draft". This is in order to avoid confusion for the reader as to the status of the document and the risk of decisions being made wrongly on the basis of the material they contain when this material may not have been formally endorsed or approved.

Staff are reminded that all work undertaken on e-mail is classed as a record and should therefore be saved on systems to ensure that it can be made available should a Freedom of Information Request require access to the information. This also includes information which may be stored on non-LPFT e-mail accounts if it relates to the business of the organisation (as used by Non-Executive Directors and Governors and other associates of the organisation).
E-mails should be stored in the record keeping system according to the business classification to which they relate i.e. e-mails related to a project should be stored with all other correspondence and documentation relating to that project. The entire e-mail should be kept including attachments so the record remains intact. Once stored in this way the original e-mail can be deleted from the person's mail box.

All electronic communication (email, faxes) should contain the following confidentiality statement and disclaimer.

This e-mail/fax and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. Therefore, if the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of the e-mail/fax is strictly prohibited. Any views or opinions expressed are those of the author and do not necessarily represent the views of Lincolnshire Partnership NHS Foundation Trust unless otherwise explicitly stated. The information contained in this e-mail/fax may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this e-mail/fax and your reply cannot be guaranteed.

Electronic Documentation Secure Storage

The Trust's network is the approved data store available for electronic documentation, which is secure and is backed up on a daily basis for business continuity purposes. All patient administration systems are stored on secure network drives. These secure network locations include the Trust Intranet SHARON, the Trust's Z Drive and individual staff members allocated H drives.

All staff should store team or service data information on designated team or service network folders which should be located on the Z drive or on SHARON as directed by local managers. Local managers will be involved in the Information Asset Management programme to ensure appropriate storage, retention and use of information held on the secure Z drive or on SHARON.

All staff are allocated personal H drives; where documents can be stored and only accessed by that individual staff member.

Staff must **never** store confidential or sensitive (or special category) data/information on their C Drive (My documents on your PC or Laptop) as this is not backed up and could also be lost because of software upgrade, failure of the PC or Laptop or if lost or stolen.

Information stored on Desk Tops are not backed up and when they are not stored on SHARON, or in H or Z drives there is a risk that this data could be lost.

Where staff use Trust approved **encrypted removable storage devices** these must be stored securely. Staff that have been allocated encrypted removable storage device will be responsible for ensuring regular data back-ups to prevent loss of data held on the device due to damage or loss of the device.

Staff must not create Access databases, excel spreadsheets or word documents to store or process multiple patient identifiable data (PID) without seeking approval from the Head of Informatics. This is to avoid duplication and to ensure the appropriate security of all patient information. The Head of Informatics maintains an accurate and up-to-date register of all data stores containing PID so that information is easily located if required and the security and access controls for the information held can be investigated and deemed acceptable.

The purpose for which we obtain and hold information as a Trust must at all times be clear and transparent. Any personal information particularly special category data should be carefully considered before being used for a different purpose to ensure that the legal basis for doing so is permitted under the Data Protection requirements. It is often unlawful to obtain personal information for one purpose and then use it for another e.g. patient information being used in a staff related matter. Advice should be sought from the Senior Information Governance Advisor or the Senior Records Management Advisor.

All records must be maintained in an orderly filing system and in appropriate secure storage which is free from unauthorised access and accidental damage. All manual records which are confidential must be kept in locked filing cabinets. Records must not be left unattended at any time to avoid inadvertent disclosure.

Tracer cards must be used to record what records have been removed from any manual filing systems showing when they were removed, the details of where they are being sent and the date that they were returned. This will allow you to ensure that you know where records are at all times. Records should be returned immediately after use to the original filing system.

Agendas, minutes and meeting papers should be stored in chronological order whether manual or electronic records.

HR files should be stored alphabetically (where two members of staff have the same name this must be highlighted on the front cover)

Where a patient/service user complains about a service it is necessary to keep a separate file relating to the complaint and subsequent investigation. **Complaint information should never be recorded in the clinical record**. A complaint may be unfounded, involve third parties and the inclusion of that information in the clinical record could prejudice the care and treatment the patient receives. If multiple teams are involved in the handling of the complaint all associated records must be amalgamated into one single record to prevent miscommunication and to aide any requests for access to the record or for sharing with the Health Service Ombudsman. This documentation must be lodged with the Patient Experience Lead.

Appendix 4

Corporate Information/Records and Folders Naming Conventions, Marking and Storage

Local decisions should be made about the directory structure and the levels and naming of folders within the directory of all records libraries.

All records must be given a unique identifier/reference and this used on all documents relating to that file.

Electronic Document Naming Convention
All electronic documents and records should be named according to the following format;
Date (in format YYYYMMDD)_File Title / Description_ Version (in format v1.0, v1.1 etc…)
For example: 20180210_Board_minutes_v2.0

Elements of the file title
In constructing a title it is necessary to decide how best to describe the informational content of the file or the individual document. The most commonly used elements in the creation of a title are listed below. It will depend on the nature of the document or folder which elements will be the most suitable for use in the title. Common elements of a title:
• Date
• Subject
• Version number

Date
The date element is essential as this will allow retention to be applied to the document or record. Using the format YYYYMMDD means that electronic files will be stored in date order.
Dates should be included to understand the content of the document e.g. minutes of meetings. (20180613_Programme_Board_Minutes_v1.0)

Subject
Where possible give your files meaningful names. This assists both yourself and other members of staff in managing and retrieving files. Always make the name of a folder or record descriptive of its content or purpose.
• Do not name the file after the person whose work it contains
• Do not use terms such as ‘general’ or ‘miscellaneous’
• Always ensure the title is: specific, consistent, sensible, understandable and helpful to others

Version Number
In order to effectively control different versions of a document it is necessary to have documented procedures. Consistent naming of different versions can be used to support version control and is useful for documents which have a number of contributors which are in various stages of development before the final version is complete. Use whole numbers (e.g. v1.0, v2.0, v3.0 etc…) to indicate finalised versions; use v0.1, v1.1, v1.2 etc…to indicate that the version is a draft and not finalised yet.

Length of a title
Titles should contain enough information in order to properly describe the contents of the document or folder. However, keeping titles a reasonable length, will help users quickly identify and retrieve accurate information.

Redundant terms
The use of redundant terms should be avoided in order to keep titles as brief as possible.

Do not use conjunctions such as ‘and’, ‘on’, ‘of’ unless they add meaning to the description e.g. Freedom_of_Information or FOI

Author
Do not use the document creator’s name in the title unless this information genuinely adds to a description of the content. This information can be added directly in the document or accessed in the document or folders Properties.

Acronyms & Abbreviations in Naming Conventions
Where abbreviations and acronyms may need to be used for naming corporate records, do not use obscure abbreviations or acronyms as they often become obsolete over a period of time and can often have more than one meaning.

Non-clinical records with specific storage requirements:

- Original agendas, agenda papers and signed minutes of Trust Board and sub-committee meetings are filed in chronological order in clearly marked files and kept in secure storage in Corporate Headquarters. These files are not to be removed. Access to these files must be directed through the Assistant Trust Secretary at Trust Headquarters.
- The Register of Interests is updated on an annual basis by the Board and is available to the public.
- The Register of Sealing is consecutively numbered and a record will be made of the sealing of every document and signed by those present when the document is sealed.
- The Register of Tendering is kept in addition to the file to which the matter relates and is available for inspection by all Directors and officers of the Trust.
- Archived Staff personal files will be requested through the Human Resources Department. It is the department’s responsibility to ensure that people accessing information are aware of their responsibilities under the Data Protection Act and appreciate professional rules of confidentiality.

When damage to records in storage is experienced, or even during the course of normal daily activity the Team Leader - Information Governance, Records and Privacy should be contacted to ensure that the records are assessed and damage identified. The Trust has a contract in place with restoration experts who can minimise physical damage to paper records i.e. water damage and this is activated by the Records Management Team. An incident report must be completed in the event of damaged records.	Records which have transferred into archive storage should be accessed following the process in Appendix 6 of this policy. Records which are stored in the archive depository can be accessed through the Records Management Team or local archiving contact.

Appendix 5

Retrieval of Physical Paper Records/Missing Records

Service identifies need for access to the records (if any) of a service user following referral, admission, complaint, claim, subject access request, third party request etc. All available electronic patient record systems checked to establish if the service user is known to LPFT services. The relevant records library should also be contacted for any historical paper records.

Requests for records held in the records library will be actioned the same working day or within 24 hours as a maximum. In an emergency records will be obtained for clinicians within 1 hour. Records libraries can be accessed out of hours by local clinical managers who have access to the appropriate security codes or keys for the departments. It should be noted that with clinical noting the majority of information being created for service users will now be available on the electronic patient record reducing the need for the manual record.

Requests for records held which have been archived will require at least 24 hours notice. The file will be returned from the external storage company on the Tuesday or Thursday following the request, to the relevant location. A signed receipt will be provided.

Where historic records are archived on CD ROM, hard drive or microfiche the Team Leader - Information Governance, Records and Privacy will arrange for the records to be made available to the requesting team either by printing the relevant records or by attaching them to the relevant record in the Electronic patient record system.

Missing records – Should be immediately reported to your line manager and this should be entered on Datix the Trust incident management system.

The service responsible for the record will conduct a thorough search of all offices and involve all staff who may have accessed the record.

Where a record has been missing for 48 hours the service will complete an untoward incident report and the records management team will investigate and update the investigation element of the Datix incident with actions taken to retrieve the record, notifications made to regulatory bodies, when a file is found and where and other appropriate contacts made to locate the record.

Movement of all any physical healthcare records should be notified to the healthcare records library.

When files are transferred between Trust teams the originating medical records library must be notified of the new file location using the fax transfer form which is sent to the records library to update the tracer.

Appendix 6

Archiving of Corporate Records

Head of Department/Team Leaders are responsible for identifying the records held by their team that are ready for archiving. This relates to files that have been inactive for over a year.

Local management files for staff who move to new LPFT teams should transfer to the persons new manager. Where staff leave the organisation the manager should review the file immediately and send any information which is unlikely to be contained in the main HR staff record to the HR department. Supervision records which are more than 3 years old and the remainder of the file should be securely disposed of. As HR files are now held electronically local managers should scan the local file and save as a PDF format and send through to jobs@lpft.nhs.uk

An annual cull of files from the office to identify files that have not been accessed for over a year (staff files for example who left over a year ago) is recommended but please also consider what you are proposing to archive in relation to the retention schedule in order that documents or files are not kept unnecessarily.

Records identified for archiving should be placed in Trust supplied archive boxes complete with lids. A full inventory record must be made of the contents of each box. A copy of the contents should be placed inside the box, a copy should be retained locally and a copy e-mailed to records@lpft.nhs.uk. The contents of a box should all relate to the same financial or calendar year (depending on the nature of the files) and have the same destruction year and this should be written clearly on the outside of each box. The box must have a tamper evident security tag affixed before dispatch from the Trust.

Access to the archiving company is facilitated through the Records Management Team.

Records which are “Not For Destruction” should be identified as such and notified to the Senior Record Management Advisor for appropriate action.

Contact the Records Management team who will arrange for collection of the boxes for archiving according to the terms of the current contract.

The Records Management Team will maintain the centrally held archiving register and will liaise with the archive contractors to determine which boxes are due for destruction according to the schedule they hold. The destruction certificates will be sent to the Senior Record Management Advisor and held centrally.

All records which do not have to be retained according to the retention schedule should be disposed of appropriately e.g. confidential information should be shredded or incinerated or placed in the confidential waste boxes. If you are unsure about whether a document/record needs keeping and if so for how long please contact the records management team.

Where HR Records are held locally by line managers and where there are staff leavers, these local HR records should be reviewed against the Trust's retention schedule to ensure appropriate information is returned to the HR Team.

Records that are held by the HR Team should be reviewed to reduce the burden of storage and for reasons of confidentiality it is recommended that a summary of HR records are held where there is not legal requirement to hold the full record (usually after 6 years from leave date)

The summary must contain as a minimum:

- Name
- Previous names
- Assignment number
- Pay bands
- Date of birth
- Addresses
- Positions held
- Start and end dates
- Reason for leaving
- Building or sites worked at.

Disciplinary case files can be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. This does not mean that there should be no record that the disciplinary process has been engaged in the main record.

Appendix 7

Archiving of Clinical Records

Paper healthcare records should be archived where a service user has been discharged from the service for 2 years. Early volumes of files may be archived and exceptions made to archive notes earlier than 2 years where space is limited.

Access to healthcare records in offsite archive store should be processed through the local team archiving contact. If you are unsure who to contact locally please contact the Records Management team for advice.

Healthcare records libraries are responsible for identifying clinical records ready for archive. Some services in the Trust have separate responsibility for archiving and team leaders are responsible for identifying records to be archived and should liaise with their local archiving contact. If you are unsure who to contact locally please contact the Records Management team for advice.

A review of files held in all locations (shelves/cabinets) should be undertaken annually to identify inactive or deceased records.

The Records Management Team will maintain the centrally held archiving register and will liaise with the archive contractors to determine which boxes are due for destruction.

Contact the Records Management team who will arrange for collection of the boxes for archiving according to the terms of the current contract. NB: The Trust no longer archives material onto CD ROM or microfiche. But access to records previously stored in this medium can be obtained by contacting the Records Management Team.

Inactive Files
Where discharged service user notes are moved to a holding area a new tracer card should be completed and placed in the library filing position to identify its storage whereabouts. These files should be placed in a TNT archive box with the original tracer card. All files kept in a holding area awaiting archive should be listed locally for ease of access.

Contents of a box ready for archiving should all have the same destruction year and this should be written on the outside of the box and the box barcode affixed. A list of the box contents should be printed off and placed inside the box. A copy should be saved locally and a copy sent via e-mail to records@lpftnhs.uk to maintain the central archive list. A standard template is available from the Records Management team.
The box barcode number should be entered onto the relevant clinical system to inform future file searches. The box must be secured with cable ties before dispatch from the Trust.

If the file has been retrieved from archive for filing purposes or general administration which does not affect the original date of inactivity of the file, then on completion of the work the file should be returned to archive store and the original date of destruction remains intact.

Clinical Records retrieved from archive for further interventions should be placed back into normal storage within the Records Library or the local clinical team location and a new tracer card commenced. The file should be notified to the archive company as being withdrawn from archive deposit (permed out).

Deceased Files
To be archived separately to comply with the retention period, archiving to occur 6 months after death. See retention schedule. Records of deceased service users where there is a serious untoward incident should be forwarded immediately to the Records Management Team and these records will be held securely at Trust HQ for 6 months or until the formal investigation has completed. Archiving will then be undertaken by the Records Management Team and these records will be archived for 10 years.

Files will be passed to the responsible clinician by the records library for them to review the file and determine whether the file has historical or research value and should therefore have a longer retention date. Tracer card to be held in the archive box in the secure holding area until file returned

If a deceased service user has early volumes in archive these should be retrieved (see retrieval section) and placed together in the archive box to ensure the entire record is retained for the appropriate retention period. The records management team must be notified of the retrieved file barcode numbers (LPF01-00XXXX) in order that they can be withdrawn and re-archived correctly

Volumes
For patients with multiple volumes of records which cannot be stored locally it is possible to send the inactive volumes off to archive store. These records must be clearly labelled on the box that they are for permanent preservation to ensure that they are not accidentally destroyed. They should have the tracer card archived with them to evidence who has previously accessed the record and a new tracer created for use in the library with the current volume.

General Advice
All records which do not have to be retained according to the retention and destruction schedule should be disposed of appropriately e.g. confidential information should be shredded or incinerated or placed in the confidential waste boxes. If you are unsure about whether a document/record needs keeping and if so for how long please contact the records management team.

During 2018/19 work will commence on creating an archive of the electronic patient administration systems so that records for inactive service users can be removed from the live patient system and placed in separate electronic storage. This work will encompass the requirement that historical records can easily be identified and retrieved by front line staff when service users represent for further interventions with the Trust, enabling access to vital historical information. However it is recognised that unwieldy patient administration systems which comprise extensive information on service users no longer active with the Trust make processing information for current service users protracted and often slow. The creation of an electronic archive will need to be risk assessed and implemented wisely to ensure that information can still be accessed expeditiously for staff who may need to access ‘old’ information quickly and often out of normal office hours.

Any system will comply with the Trusts retention schedule to enable the organisation to only hold information for as long as it is needed and then dispose of that information when it reaches the end of its retention period.

Appendix 8

Transporting Information, Records and Equipment

Agile/Mobile Working

Mobile working presents a very real risk to the security and integrity of the Trust's information. Moreover the legislation which surrounds the way in which the organisation uses and is responsible for information makes it liable for any breach or failing in security. From patient information held in paper records or on laptops, to the contact details on a mobile phone to the financial spreadsheet e-mailed to a home PC, the inherent risks to information should be apparent to all staff. By recognising that the risks exist, and by implementing the controls set out in this policy, the Trust and its staff will aim to play their part in controlling them at a manageable level.

All staff wishing to work 'off-site' must have this authorised by their line manager using the relevant form in the staff handbook

DO

- ✓ Ensure that if connection to the Trust's Computer Network is required that the appropriate authorisation is in place
- ✓ All equipment/devices MUST be encrypted before use.
- ✓ Ensure that the password security option is turned on and a strong password set refer to the guidance contained in the associated policy Information Management and Security.
- ✓ Set the equipment to power-off after a pre-determined period.
- ✓ Ensure all reasonable steps are taken to ensure that the equipment and information is not misplaced or stolen
- ✓ Store information & portable computer equipment away securely whenever it is not in use. This should be in a locked cupboard or cabinet.
- ✓ Transport portable computer equipment in non-identifiable containers
- ✓ Transport information and equipment in car boots out of view, removing from the car immediately on arrival for use or secure storage in a building.
- ✓ Log-off when moving away from the equipment
- ✓ Regularly connect the device to the Trust Computer system to update the anti-virus software.
- ✓ Regularly back-up data onto the Trust network.
- ✓ Obtain authorisation prior to the removal of information and portable equipment from the premises.
- ✓ Report any missing information and portable equipment on the Incident Risk Management system and to your line manager and the police if appropriate.
- ✓ Do routinely clear the memory on sat navs which may contain addresses for service users.

DO NOT

- ✗ Leave information & portable computer equipment unattended
- ✗ Leave information & portable computer equipment in places where it can be easily stolen
- ✗ Leave information & portable computer equipment visible in the car when travelling between locations
- ✗ Leave information & portable computer equipment visible in an unattended car
- ✗ Leave information & portable computer equipment in the boot of a car for long periods of time or overnight
- ✗ Put the information & equipment down on the ground or on a counter beside you when in busy areas such as bus stops, railway stations or if travelling on the London Underground
- ✗ Leave the information & equipment visible through windows at home
- ✗ Install unauthorised software or download software/data from the internet
- ✗ De- Activate the anti-virus software
- ✗ Remove information & portable computer equipment from Trust premises without authorisation
- ✗ Access Confidential information from portable computer equipment not owned or managed by the Trust.
- ✗ Store Confidential information onto unencrypted portable computer equipment under any circumstances.
- ✗ Allow any unauthorised person to use the equipment
- ✗ Log on to the Trust's computer network other than via the Remote Access Server/VPN.
- ✗ Email Confidential Information to or from a home or personal email address.
- ✗ Use encrypted removable storage devices for routinely transferring information between sites.
- ✗ Allow unauthorised individuals to see confidential information whilst you are working on it at home or other location.

Appendix 9

Clinical Coding

In 2017/18 the Trust contracted an external provider to undertake the clinical coding function inpatient episodes. The contracted provider will provide on-site clinical coding on at least two occasions within each month and comply with the legal requirements set out within the contract document.

Trust's Responsibilities

24 hour discharge/transfer notification form is to be completed by the inpatient medical staff on the following occurrences:

- Discharge from an inpatient bed
- Transfer to another in-patient area or alternative psychiatric healthcare provider
- Change of Lead Consultant
- Death of the service user

This should include as much designated information as possible including the primary and all secondary diagnoses as well as mandatory co-morbidities. Any procedures undertaken such as ECT should be included.

24 hour Discharge/Transfer Notification Form will be communicated electronically to the GP. The original is to be scanned and attached onto the relevant clinical system within the discharge summary folder of the document section. **The contracted Clinical coders should use this form for assigning the initial diagnosis coding and input the researched and indexed ICD 10/11 codes into the electronic patient record system at the next on-site visit to the Trust following the discharge/transfer.** Please note where ICD 10/11 codes have been included in the discharge/transfer form; these should be checked against the ICD 10/11 manual for accuracy.

The Performance department will monitor the in-patient turnover using the standard FCE report on the clinical system. Any discharges that have not had a 24 hour Discharge/Transfer Notification Form uploaded onto the clinical system within 3 working days of discharge will be escalated to the relevant ward manager and the Lead Consultant. If the discharge/transfer has still not been communicated according to the above process within 5 working days of the discharge/transfer then further escalation will be made to the Clinical Director and the relevant Service Business manager to resolve.

The Full Discharge Summary: The full discharge summary letter should have been completed within 2 weeks of discharge. The Lead Consultant's administrative support must ensure that a copy of the full discharge summary is sent electronically to the relevant GP and that it is scanned and attached within the discharge summary folder within the document centre of the electronic patient record. The Performance department will monitor compliance and provide reports on performance against timeliness and completeness.

The Clinical Coder will check the diagnosis on the discharge letter against those already coded on the system. Where there is a discrepancy clinical coders should liaise with the Consultant concerned and any changes made to the codes should be documented on the coding amendment form and signed off by the Consultant and scanned and attached to the document centre. Any necessary changes or additions will be made to the coding module on the electronic patient record system.

The clinical coders will also thoroughly check the electronic healthcare records to identify any of the mandatory co-morbidities and assign the relevant ICD10/11 code onto electronic patient

record. The mandatory co-morbidities are catalogued in the Connecting for Health Coding Clinic newsletter.
http://www.connectingforhealth.nhs.uk/systemsandservices/data/clinicalcoding/codingstandards/publications/ccmarch2010.pdf.

The Performance Officer with clinical coding lead responsibilities will act as liaison between the Trust and the contracted clinical coding service and will report activity and compliance to the IM&T Committee through the Data Quality Group. Clinical Coding Standard Operating Procedure and Guidance is available by contacting the Data Quality Group.

On a monthly basis the Performance department will provide performance reports detailing timeliness and completeness of the Trust's clinical coding. In addition the Trust will commission an annual external audit of the Trust's clinical coding processes to inform the Data Security and Protection Toolkit.

Contracted Clinical Coding Providers Responsibilities

The contracted Clinical coding provider will ensure that their clinical coding staff are trained to national clinical coding standards and receive access to ongoing refresher training to maintain their competencies to ensure Data Security Protection Toolkit audit requirements are maintained at a high level.

In addition, as per terms of the contract, the clinical coding provider will ensure that the quality of the coding will be maintained to ensure that Data Security Protection Toolkit audit requirements are achieved and maintained throughout the period of the contract.

Appendix 10

Data Quality Checks and Correcting Errors

The Informatics Team will run data quality checks against specified data items in accordance with all mandated national data sets as contained within the clinical information systems used by the Trust to check for validity, reliability and completeness. Data quality reports will be made available to relevant service managers/business managers to monitor and take corrective action to ensure that data quality improves.

A programme of weekly and monthly error reports/missing data reports from the clinical information systems reports menus are available for teams to run on a routine basis for self audit and correction. Additional reports created by the performance team and Informatics Team will be assessed and all data quality issues identified with the appropriate department or entering staff for rectification.

Investigation of external Data Quality reports such as the secondary uses service will be reviewed by the Informatics Team and shared with the services for action and improvement.

The Informatics team will undertake validation tests on the quality of the data submitted for the Mental Health Services Data Set and the Commissioning Data Set as required on monthly and quarterly basis to ensure that the information submitted is error free and does not cause submission rejection.

To enable the Trust to ensure that information and data quality issues are dealt with in a co-ordinated way, the Data Quality Group produces an annual action plan to target specific issues with recording and consistency of standards:- This will ensure:-

- Core work is carried out to improve the quality and timeliness of data collected
- Establish consistency with data definitions and use of information
- Support services in maintaining data quality to deliver local and national initiatives
- Facilitating audit on adherence to national standards
- Ensuring that upgrading or renewing clinical information systems does not impact on effective recording of information for management or clinical purposes

Appendix 11

Scanning Paper Documents – Protocol for scanning processes

If a department/service considers that it may have paper copies of LPFT owned non clinical documents which may be more appropriately stored as electronic documents. They will be required to develop and document local processes for the scanning of these documents. These will need to be based on the operating and procedure manual of the electronic system it is planning on using. They will need to follow guidance on Appendix 12. (this will NOT apply to documents bearing the Trust seal, contracts, title deeds, original plans or leases).

Head of the Department must undertake a risk assessment of the proposed departmental procedure against the process detailed in the next page. This risk assessment will identify areas where the departmental procedure deviates from the recommended process. Weighting in regards to risk should then be considered for the deviations and potential methods of resolution identified and costed. This process should take into consideration the views and recommendations of external bodies, NHS bodies such as NHS Improvement, auditors, and technicians.

Proposed departmental procedure, full risk assessment and potential resolutions or mitigations of risk submitted to Information Governance and Records Management Group for approval and onto IM&T Committee for sign off and approval.

Once the proposed process is ratified departmental scanning process can commence.

For clinical documents each clinical system in operation for the Trust has the functionality to scan/attach documents to reduce the reliance on legacy paper records. Each system has a local operating procedure for the scanning process to be applied in their particular speciality.

Appendix 12

Scanning Corporate Paper Documents

Paper document enters Trust from external source / internal document is complete (once all required signatures, notations etc. have been added). Document date stamped and initialled.

Decision made that document needs to be retained and for how long in accordance with retention schedule. (See Appendix 23)

Trust Multi-Functional Devices (MFD's) should be used to scan documentation.

Full compliance with The Code of Practice 'BIP 0008-1:2008: Evidential weight and legal admissibility of information stored electronically. This requires that documents should be examined prior to scanning to ensure their suitability. Such factors as their physical state (thin paper, creased, stapled etc) and the attributes of the information (black and white, colour, tonal range etc.), the number of pages, the type of material and whether the document is itself a copy should be noted. The Trust MFD's comply with this requirement.

A unique identifier should be assigned by following the Trust naming conventions.
(See Appendix 4)

An audit test will need to be carried out to ensure that the quality of the scanned document, in terms of legibility, resolution, thinline detection, coverage of A4 page, dimensional accuracy and greyscale detection is maintained. Only if the test proves satisfactory should the batched documents be scanned. If there is a problem a record should be kept of the problem and how it was resolved and reported to the Information Governance and Records Management Group.

Scan documents and ensure a record of date, time and individual scanning done automatically by the electronic system and attach into the electronic record.

An audit of the document scanned into the system should be undertaken to ensure that the documents have been scanned according to protocol. Then the original paper documents should be identified as scanned and a true copy of the paper record is held electronically by the verifier and can then be destroyed.

Appendix 13

Scanning Paper Documents for Electronic patient records

As part of the process to change from a joint paper and electronic record to a paper light record the Records Team have created a document centre scanning and filing spreadsheet listing all documents that should be scanned/ uploaded and filed or destroyed confidentially for each clinical area. MHA Documents should be scanned within 24 hours and notified to the Mental Health Act team; all other documents should be scanned and uploaded within 3 working days.

Please ensure you have the NAPS2 scanning icon on your desktop. (If the icon is not installed, then please contact it.supportdesk@gemcsu.nhs.uk and request that NAPS2 is installed).

MFD's are now used Trust wide and provide a scanning solution for single or multiple scans per patient, using the Smart Scan function. Use Safecom to retrieve your scanned documentation. Access SafeCom from the SHARON homepage and click on **Print Qs at Trust** and click on **Safecom Admin Scan to me documents**. Select Documents/Files to view your scanned document/s and Save to the S Drive. Download documents within 2 days before they are deleted from Safecom.

Before scanning your document:

- Check for readability and clarity of the print.
- Ensure there are no staples or paperclips attached to the document.
- Check to see if the document is double or single sided.

If the document is a Mental Health Act form on coloured paper, consider scanning in colour (by changing the settings on the scanner)

Scan your document according to the clinical system training guide, following the naming convention: YYYYMMDD_Document_Title_Other_Description

Titles should contain enough information in order to properly describe the contents of the document to help system users to quickly identify and retrieve accurate information. The date will refer to the date the event or appointment occurred. For example: 20180613_Outpatient_Letter_Dr_XXXX.pdf (use underscore and not spaces)

Scanned documents should always be saved as a .pdf document. Upload your document onto the S Drive.

Log into the electronic patient system and upload your document from the S Drive according to the clinical system training guide, ensuring you have set patient focus on the correct patient. You can change the name of the document from within the document centre in the clinical system, after the document has been uploaded and according to the correct naming conventions above.

Check the quality of the scanned document and ensure it has been uploaded to the correct patient.
If the document is of a poor quality or unreadable, re-scan, altering the properties.
If the document has been uploaded to the wrong patient log a call to the IT helpdesk to have it removed and then attach to the correct patient.

Do not stamp or alter MHA paperwork or legal documents.
Add original MHA section papers to the physical paper file and return to the MHA team when appropriate. Add original medication cards to the physical paper file.
All other scanned paper records can be shredded once quality checked on the clinical system.

Appendix 14

Sharing Information with Staff involved in the treatment/care of the Service User

Information should only be released on a 'need to know' basis. (Do not talk about service users in public places or where you can be overheard.) Reasons might include: ensuring the views of the service user are known, for assessment, discharge and review purposes, to enable professionals to give/gain clear advice on specific problems, to avoid duplication or omission, to facilitate joint working, to assess the relevance of referrals and subsequent allocations, to ensure staff are aware of risks, to promote positive outcomes for the service user, or to identify risks to children and young people or vulnerable adults.

Sharing Information within a team

White boards and name boards above inpatient beds and in other areas should only state the service user's name (initials preferably) and if the service user insists that they do not want their information displayed in a visible public area you must respect their decision.

No other service user identifiable information should be put onto whiteboards located in public areas, for example address, date of birth or specific clinical details.

If it is absolutely necessary to put clinical information onto a whiteboard not located in a public area, the information should be abbreviated or symbolised so as only health professionals can understand the information and no other members of staff or visitors that may come into the department.

Sharing Information by Post

All correspondence containing PID must be addressed to a named recipient and marked 'Private & Confidential' or 'Addressee Only' as appropriate.

When sending out information in the post where the recipient may not be clear as to the identity of the originator, staff should ensure that either a Compliments Slip is included or that the enclosure clearly states the name, title and contact details of the sender.

Double envelopes should be used for particularly sensitive (or special category) information and a tamper proof envelope for healthcare records.

The internal courier can be used for sending PID but the courier requires that the full postal address is used on all envelopes and bags, courier numbers are no longer in use.

Royal Mail Special Delivery should be used for large quantities of PID sent externally (i.e. copies of healthcare records). Original healthcare records **must never** be sent outside the Trust.

All information sent on portable media must be encrypted before being sent by Special Delivery.

Receipt of information should be confirmed using the file receipt form.

All incoming post should be opened away from public areas and by the addressee or designated personnel only.

Sharing original and photocopied healthcare records or HR files

Only the approved records courier bags or boxes should be used to transport/post records secured with tamper evident seals. Where bags are unavailable the approved process is to utilise doubled envelopes securely sealed. Records must always be accompanied by a file receipt sheet so that the addressee can confirm safe receipt of the file.

Sharing Information by Fax
Always use the fax cover sheet. All faxes to contain the disclaimer outlined at appendix 3 (This forms part of the Fax Cover Sheet)

1. Non-Safe Haven Fax:
2. Remove PID from any fax unless it is absolutely necessary.
3. Personal details should be sent separately to clinical details (which should be identified by NHS number only).
4. All correspondence containing PID should be addressed to a named recipient and marked 'Private & Confidential' or 'Addressee only' as appropriate. Complete fax header TO, FROM, contact numbers and number of pages
5. Telephone the recipient of the fax to let them know you are going to send.
6. Always check the number to avoid misdialling.
7. If possible obtain transmission report from fax machine.
8. Confirm with the recipient that they have received the fax.
9. If your fax machine stores copies to its memory, ensure that the memory is cleared.

Safe Haven Fax:
Safe Haven faxes are those located in a secure and private area which is locked when unattended.
Steps 2 & 4 above are not required. Other steps should be followed. The list of safe haven faxes is updated on an annual basis by the Senior Information Governance Advisor.

Sharing Information by Telephone
Verify the identity of the caller by checking the telephone number and calling them back.
Do not leave messages on answer phones containing clinical or confidential information. Simply leave your name, a telephone number and a request for the individual to give you a call back. It is best practice to gain consent from the service user in advance to establish if they are happy for you to leave a message. Document this on the electronic patient record.

Where a member of staff is unsure regarding a request they should consult with their line manager. If any doubt remains the team leader or ward manager should liaise with the Records Management Team.

Appendix 15

Request from Partner Organisation/Third Party/Individuals Acting on Behalf of Service User

All Service Users should have been made aware at their first point of contact with the Trust and at regular intervals thereafter (at least annually) of the ways in which their information may be used and the situations in which it may be disclosed. It is reasonable to assume that most (if not all) of the information provided by service users is confidential in nature. Check the information sharing consent completed by the service user which identifies whether or not the requestor has permission from the service user to access/be party to their information. See appendix 1.

Requests for access to information may come from:

- Relatives, carers, persons acting on behalf of the service user
- Police (do NOT have an automatic right to personal information)
- Solicitors (do NOT have an automatic right to personal information)
- Courts
- Other NHS Trusts/Other statutory agencies
- Third sector/ private or voluntary organisations
- Private individuals following the death of a service user

All requests for access to records must be made in writing and should be sent through to the Subject Access Team. The only exception may be in Safeguarding Children or Vulnerable Adults situations where urgent information sharing is required. The principles of necessity and proportionality should still be adhered to and the Trust Safeguarding Team should be consulted. Requests for non-confidential information should be treated as Freedom of Information requests and sent through to Corporate and Legal Services. All requests for information from the media should be directed to the Communications department. Other staff should not provide any information.

The Subject Access Team will determine if there is sufficient lawful authority for the disclosure (e.g. Court Order, service user consent or appropriate Police form to include Data Protection schedule identification signed by a police inspector or above) in accordance with the Data Protection Act 2018.

They will liaise with the requestor to determine the authority of the requestor, the purpose of the request and which records are being requested and determine if there is a valid legal basis for the disclosure.

The Subject Access Team will also involve the appropriate consultant, practitioner or care co-ordinator to determine their opinion on the content of the notes and the appropriateness of release as the clinician(s) may limit or deny an individual's health record request under the following two reasons:-

- where the information released may cause serious harm to the physical or mental health or condition of the service user, or any other person
- Or where access would disclose information relating to or provided by a third person who had not consented to that disclosure and where their consent cannot be bypassed on the grounds of a greater public interest. Information about third parties should be anonymised wherever possible so that the individual cannot be identified.

They will also ask the clinician(s) whether they think it would be possible and/or appropriate to seek the service user's consent for disclosure (including whether the service user has the capacity to consent and if not if there is someone with lawful authority to consent on their behalf).

Where requests have been made by those with parental responsibility the Subject Access Team should discuss with the relevant clinician whether the child/young person is competent to make decisions about the sharing of their record. Parental access to the records may be denied where:

- Granting access would be likely to cause serious harm to the physical or mental health or condition of the child
- Granting access would disclose information provided by the child:
    - In the expectation that it would not be disclosed to his/her parents
    - As a result of any examination or investigation to which the child consented in the expectation that the information would not be disclosed

The minimum information, as is necessary, to fulfil the purpose should be disclosed. Depending on the reason for the request for information it may be possible to provide anonymised data, which does not identify individuals. This should be done wherever possible.

Where a member of staff is unsure regarding a third party access request they should consult with their line manager. If any doubt remains the team leader or ward manager should liaise with the Subject Access team who will liaise with Corporate and Corporate and Legal Services if necessary. Ultimately the decision whether to release will rest with the Caldicott Guardian.

The Subject Access Team will inform Corporate and Corporate and Legal Services of any requests where there is an indication that a claim will be made against the Trust or any pre action protocol request forms received.

Where information needs to be shared in an emergency situation (Safeguarding Children or Vulnerable Adults, Police requests where the safety of the service user is in question) the identity of the requestor should always be confirmed (verify telephone numbers and call back, request ID etc). For police requests for access to information in an emergency the protocol in the memorandum of understanding with the police for Police Health Based Place of Safety (previously S136) requests should be followed and where there is concern this should be discussed with the Team Leader – Information Governance, Records and Privacy/Caldicott Guardian or raised to the attention of the on-call manager out of hours.

Solicitors do not have an automatic right to demand access to their client's notes on the ward. Where solicitors wish to view notes to prepare for Mental Health Act review tribunals, appeals or similar legal proceedings they must make a formal request through the Subject Access Team.

The form Informal request for access to healthcare records Part A should be completed by the service user and handed to ward staff for forwarding to the Subject Access Team detailing the name of the representative who has permission to access their notes.

On receipt of the form the Subject Access Team will liaise with all parties to ensure that the access can be facilitated by the ward or at Trust HQ.

Access to the Records must be supervised at all times by a member of the ward staff or records team. Records must be checked for third party information and information not to be divulged prior to the appointment taking place and information not to be shared should be removed. On completion of the informal access ward staff to forward completion of informal access Form B to the subject access team to confirm access has been complied with.

Appendix 16

Contractual Arrangements with Partners

Where information is to be routinely shared as part of a contractual arrangement to provide services, there is a clear expectation that partner organisations will maintain the same levels and approaches to information security as the Trust. Each partner organisation has an information sharing memorandum of understanding with the Trust and these are reviewed and updated annually to ensure that they are legally robust. Memorandum of Understanding.

Where individuals from outside the organisation will be accessing the Trust's Electronic patient records or will have access to paper-held information, contracts must be in place before access is allowed. These contracts will ensure that the external body will comply with the appropriate confidentiality and security procedures. This contract may take different forms depending on the nature of the function the external individual/organisation is carrying out (e.g. IT services, window cleaning, research).

Arrangements will be made with Mental Health Act Inspectors, CQC Inspectors, External Auditors and other NHS inspectors to have access to both electronic and physical healthcare records to enable audits to be undertaken on the functions of the organisation. Access to the records will at all times be supervised and will be conducted on a strict need to know basis.

Appendix 17

Subject Access Request (Service User)

The Data Protection Act 2018 gives every living person, or their authorised representative, the right to apply for access to their health records or to obtain copies.

Does the service user wish to have a copy of their record or simply to access their record (i.e. look at it on the ward whilst they are an in-patient)? (this may include images of them on CCTV). If they require a copy service users should be informed that the request will need to be in writing or they can use the Subject Access Requests form available on Access to health records

Formal Access (copy of records) Forward written request using either the form or a letter from the service user to the Subject Access Team or direct service user to the email address for on-line requests records@lpft.nhs.uk and lpn-tr.lpftrecords@nhs.net	Informal Access (viewing of records) Facilitated by local staff or the records team but Subject Access team informed for recording purposes and informal subject access form part A completed and sent to Subject Access Team

Is there sufficient information to verify the identity of the service user and locate the information they require? Has sufficient legal authority for disclosure been provided (letter or access request form signed by service user.

Log applicant request and comply promptly, within 30 days of request. In exceptional cases it may take longer. If it appears likely that compliance will take longer, the applicant should be informed and an explanation of the delay provided.	Subject Access team contacts requestor asking for necessary consent/evidence of lawful authority, more information to locate required information or necessary fee.

Subject Access Team emails via outlook an approval memo to ensure the health professional has considered the request, as under the Data Protection Act 2018, they may limit or deny access to an individual's health record request:- • where the information released may cause serious harm to the physical or mental health or condition of the service user, or any other person

The Trust need not inform a service user that it is holding personal data about him/her for the purposes of the prevention or detection of crime or to apprehend or prosecute offenders. Nor does it have to inform a service user that information has been provided to or received from another organisation for these purposes (e.g. the Police)
Deny access or provide the service user or their representative copies of the relevant parts of the health records, or alternatively, set a date for them to view the relevant records once the fee has been paid. If copies are posted they must be sent special delivery. A meeting can be arranged to discuss the records. This should be the norm where information is to be disclosed of which the service user was not aware, or where it is likely to cause upset or distress.

Where informal access takes place in a ward or team setting practitioners are responsible for checking the records before sharing to ensure that third party and confidential information is removed. The service user must be supervised at all times while informal access is being conducted. On completion of the access appointment the completion of access form part B should be completed and sent to the subject access team.

If a service user is unhappy with anything written in the records they can challenge this. The Subject Access Team will ask them to complete a challenge to content of records. The challenge will be considered by the Trust and where appropriate a comment will be added to the original entry in the healthcare record directing staff to take into consideration the comments of the service user or the record will be amended.

If a service user is unhappy with any aspects of the access request, try and resolve locally with the Subject Access Team. If this is not an option explain the NHS Complaints procedure or alternatively direct them to the Information Commissioners Office.

All documentation to support subject access requests is available on the Trust website for service users to access the relevant request forms Access to health records

Appendix 18

Subject Access Request (Staff Member)

The Data Protection Act 2018 gives every living person, or their authorised representative, the right to apply for access to their personnel/HR records/Trust records or to obtain copies.

All requests for access to personnel/HR files should be directed to the Records Management Team who will liaise with local managers and Human Resources to identify the information held on the individual in whatever medium it is stored.

Is there sufficient information to verify the identity of the staff member and locate the information they require? E.g. request via Trust email or in person the ID badge is checked.
Has sufficient legal authority for disclosure been provided (letter or subject access form) signed by staff member/ evidence of court's appointment/ evidence that individual has claim)?

Log applicant request and comply promptly, within 30 days of request. In exceptional cases it may take longer. If it appears likely that compliance will take longer the applicant should be informed and an explanation of the delay provided.

The Trust need not inform a staff member that it is holding personal data about him/her for the purposes of the prevention or detection of crime or to apprehend or prosecute offenders. Nor does it have to inform a staff member that information has been provided to or received from another organisation for these purposes (e.g. the Police) The Trust need not inform staff members if requests for information have been met from statutory or professional bodies i.e. NMC in the interests of patient safety.

Records will be reviewed and initial Data protection checks on the contents undertaken by the Records Team in conjunction with HR and local manager. Final Data Protection checks and any redactions necessary to maintain confidentiality or minimise harm or distress to the staff member will be undertaken by the Subject Access Team.

Subject Access Team to arrange dispatch of copies of records on completion of all checks.

Deny access or provide the staff member or their representative copies of the relevant parts of the records, or alternatively, set a date for them to view the relevant records.

If a staff member is unhappy with anything contained in the records they can dispute this with the HR Department.

In general the Trust will not send Personnel/HR records to another organisation following the transfer of a member of staff. However in the case of a TUPE transfer between health and social care organisations it is possible that personal files will be shared, where there is clear evidence that this will be to the advantage of both the organisation and the individual transferred. The decision to transfer information will rest with the Head of Operational HR and in line with TUPE regulations 2006.

Where applications are received under Freedom of Information for access to Personal Information the Corporate and Corporate and Legal Services Department will acknowledge receipt of the request and then forward the application to the Subject Access Team so that it can be dealt with in accordance with Subject Access provisions. The original date of receipt will be the date used for working to statutory timeframes for release.

Appendix 19

Requests from Family/Friends for "Update" on Service User

Family member/ friend of a service user makes contact with staff requesting an update on the service user's condition/well being etc. Remember that even the fact that someone is a service user or that they are in hospital is confidential

Check the identity of the requestor.

Check the confidentiality and consent form completed by the service user which identifies whether or not the requestor has permission from the service user to access/be party to their information. (See Appendix 1.)

Has the service user expressed their wishes and feelings regarding this family member/ friend receiving information about them?

Act according to the expressed wishes of the service user.

Where possible/appropriate ask the service user if they wish you to share any information with the individual.

Where a service user lacks capacity to make a decision regarding sharing information with their relatives the professional should decide whether they believe it is in the service user's best interests for information to be shared.

A record should be made of the believed lack of capacity and the rationale for disclosure in terms of best interests and what information was shared.

For example, in the situation where a service user is unwell and decides that previously involved family members/carers cannot be updated with information, give careful consideration to what information can be shared to reassure.

Check the history of information sharing decisions. Think about who is going to be supporting the service user in the community on the road to recovery. What is in the patient's best interests?
It might be appropriate if the family are updated with generic information which assures them of the service user's wellbeing and safety without giving specific information. A conversation could start with "I cannot divulge much information as I do not have consent but I can tell you that the service user had a settled night/patient is due to see the doctor later/service user is due to be visited later".

Where a member of staff is unsure regarding a request they should consult with their line manager. If any doubt remains the team leader or ward manager should liaise with the Subject Access Team. Final Decisions on whether or not to share information will rest with the Caldicott Guardian.

Appendix 20

E-mail/Text and Telephone Exchange with a Service User

Guidance for Email/Text

Has the service user requested email/text contact or has a need for email/text communication been established?

The risks and benefits of email should be explained as per the Confidentiality and Consent Form

Health care professional should discuss with the service user to explain the email/text facility and answer any questions. The following 2 points should be specifically explained:

- The service user should be cautioned to take care compiling their messages to NHS staff as email/text carries the same weight in law as the written word and the authority of the sender.
- Email/text should not be used for urgent messages, such as reporting a crisis. In situations where contact needs to be made urgently, service users and carers are advised to use an alternative direct method e.g. telephone.

The service user should be asked to sign the Confidentiality and Consent Form. This should be scanned onto the electronic patient record and the original should be given to the service user.

If there has been **no** discussion with the service user then exchange of information by email/text should **not** be considered at this time, unless the service user has instigated the exchange.

All email communication with service users should be cut and pasted into the electronic patient record. The email should then be deleted from the staff member's inbox/sent items.

When texts are sent to or received from a service user a record must be made in the clinical notes of the time and date and content of the text. The text can then be deleted.

Any potential, suspected or known breaches or inappropriate use must be reported immediately to the Information Governance department for advice. Any identified information security incidents or risks should be reported on the Datix incident management system.

Guidance for Telephone Exchange

Receiving and making calls:
Health information is legally defined as 'sensitive' and 'special category' under Data Protection. Therefore we need to ensure we provide a confidential service, protect information and Inform patients of how their information is used. We need to provide choice to the service user so that they can decide whether their information can be disclosed or used in particular ways.

There are many examples where information has been given to an inappropriate person or in extreme circumstances impostors have been able to obtain sensitive patient information.

A patient has a right to privacy so we must talk to the service user, unless we have a justified reason to speak to someone on their behalf, e.g. they have given their consent or it is in their best interests.

Unless you can guarantee that the message will be delivered to and received by the correct service user then do not leave a message.

Whether the service user is happy for staff to leave messages on a telephone answer machine if necessary.

Calls to/from staff involved in care of patients
Always confirm who you are speaking to before releasing information. If someone has called you and you are not sure who they are, if possible, ring them back through a switchboard.

Health professionals and carers may need to know information to provide best care for the patient, but you may need to provide it without consent in circumstances that warrant it, the key is thinking about it and documenting actions taken.

Calls to/from relatives/friends/others
Confirm information; get the caller to tell you things about the patient to validate their legitimate rights to the data which confirms you are talking to them about the right person.

When calling someone at the request of the patient, or because they need to be contacted always try to speak directly to them without releasing information to whoever answers the phone.

Leaving messages on Answerphones:
Patient confidentiality can be breached from messages left on answer phones, resulting in embarrassing or harmful situations arising.

The following points offer guidance about this;

- Before leaving a message consider the urgency of getting the information to the patient. If it is not urgent and another attempt to speak to the patient can be made, do not leave a message.
- If you feel you have to leave a message, think about what you say, and leave the minimum amount of information – for example, 'Please call (number) to talk about your appointment' (This will be clear to the patient, but ambiguous to anyone else hearing the message.)

The possible dangers of leaving messages:
If you leave an answer phone message, the service user may not be the first to hear the message. Please do not identify the Trust or leave any clinical information.

Please consider:

- Who might hear the message?
- Are you sure you have called the correct number?
- Will the recipient fully understand the content of the message?
- How can you be certain the message has even been picked up?
- Will you inadvertently breach confidentiality?

When the phone is answered by someone else:
Always ask to speak to the patient, but don't say where you are calling from initially.

If they ask who is calling, you should respond with a minimum amount of information. Stating you are calling about their appointment may be sufficient. If they continue to ask where you are calling from, only tell them if the organisation name does not imply anything to do with the health of the patient.

If the patient is not present, then unless there is a degree of urgency do not leave a message, but request a suitable time to call back.

Appendix 21

Sharing Letters with Service Users

At first contact staff should provide service users with a copy of How we How we use and share your information to help you leaflet. The limits of confidentiality should be discussed with the service user. (See Appendix 1). Service users can be directed to the Trust's website for more information on how their information is held securely.

A copy of all Clinicians' letters, therapeutic letters, referral letters, discharge letters, care plans will normally be provided to the service user. This should be discussed with all service users (including 16 and 17 year olds) at their first contact with services and their preferences recorded on the confidentiality and consent form. If a service user currently does not have a completed form one should be completed at their next contact. The following should be discussed and confirmed with the service user:

- Where they would like to receive the letter (alternative address, collection point etc.)
- In what format they would like to receive the letter (large print, audio cassette, electronic file etc in line with the Accessible Information Standard and Data Protection rights.)
- In what language they would like to receive the letter (including symbols or Braille)
- If they would like anyone else to receive copies of the letters (carers/relatives etc.)

Where the service user does not have capacity to consent to receiving letters the professional will have to decide (unless there is a Lasting Power of Attorney or Deputy with this authority) whether it is in the service user's best interests to receive the letters themselves or possibly for them to be sent to a carer/relative. For service users under the age of 16 professionals should determine the capacity (Gillick or Fraser competence) of the service user to decide whether they wish to receive copies of letters and if others should receive copies. Where there is more than one individual with 'parental responsibility' it is important to discuss who should receive copies.

The Consent Form should be filed in the confidentiality statement section of the document centre.

Contact had with service user that generates the need for correspondence with another professional. Service user reminded of any stipulations on their Confidentiality Consent Form and any adjustments made.

All correspondence to other professionals generated by Trust staff should be typed on Trust headed paper. The NHS number should be recorded on all correspondence. It should be documented on the letter who it is copied to (c.c. at the bottom). Jargon should be avoided. Where medical/professional terminology is a necessity, an explanation of this should be given either in the letter itself or at the consultation. Where staff are unsure of the appropriate layout for clinical letters they can either utilise the letters facility in the electronic patient record or make use of the letter template. Trust guidance on electronic document naming conventions should be followed for Clinical Letters (See Appendix 4)

Healthcare professional writes to GP or other professional (there is nothing to stop the healthcare professional writing to the service user and copying in the GP or other professional).

Letter either copied directly to the service user or the healthcare professional may feel that it is necessary to remove certain information where:

- It is personal data which identifies another person, unless that person has consented to the disclosure or can be fully anonymised or it is reasonable to provide the information without consent.
- It is likely to cause harm to the physical or mental health or condition of the person to whom the letter relates or another person
- The service user has indicated they do not wish to receive copies of correspondence or wish to have information communicated by another means (this should be clearly recorded in the healthcare record in the section on correspondence using confidentiality and consent form

The staff member typing the letter **must** check the address and name of the person receiving the letter on the Confidentiality and Consent Form. Where an alternative format is required this should be arranged (the Communications department can advise in respect of translation services/accessible information standards)

All letters with clinical content must be authorised by the author via a signature. Where it has been determined by Service Managers that an **electronic signature** process is required then services will be able to access to the use of Trust approved digital dictation devices for the creation of clinical letters and clinical approval as part of the clinical/electronic signatures process.

Where this is not in use the member of administration staff will create the clinical content letter for the clinician. They will then email the clinician for authorisation of the content. The clinician will respond via email to approve the content of the letter, which will then enable the approved electronic signature to be applied as sign off. This email will be scanned as a record of audit for approval of the content of the letter, along with the signed letter into the patient's record.

A signed copy of all correspondence should be scanned and uploaded to the electronic patient record.

The envelope in which the letter is sent should be marked **'Private & Confidential'**.

Appendix 22

Freedom of Information Act Requests

All requests for information that are not patient specific (i.e. relating to confidential information about patients) or staff specific (i.e. relating to confidential information about staff) are considered to be requests under the Freedom of Information Act, even if they do not specifically say as much

An FOI request must be: in writing, state the name of the requestor and a return address and describe the information requested. Anyone wishing to make a request should be informed of these requirements and given the Corporate and Corporate and Legal Services address or Trust FOI email (FOIrequest@lpft.nhs.uk)

Staff member receives a request for information and follow the process below:

Immediately forwarded to Corporate and Corporate and Legal Services	Is the FOI request clearly a 'round robin' request? If YES Corporate and Corporate and Legal Services to alert partner FOI leads.
Corporate and Legal Services send acknowledgement to the FOI Requester within 2 working days of receipt.	
Corporate and Legal Services check that there is a name, contact details and that the request for information is clear.	

Corporate and Legal Services check whether the request has been asked for previously by this person or if information requested is similar to a previous request by this person.	Is FOI Request repeated/vexatious?	Issue a refusal notice
Corporate and Legal Services forward the request as soon as possible onto the appropriate department – requesting information as soon as possible and giving deadline for feedback.	Does department require clarification on request?	Corporate and Legal Services seek clarification from the requestor

Log the FOI request on the FOI Request Log. • Recording the date it was received • the name and contact details of the Requester • Brief description of information required • Date acknowledgement letter sent • Name of persons and of department request sent to (and date sent to the dept) • Date the FOI request is due by (a response is required within 20 working days)	Where the FOI request is clearly a subject access request for personal information held or holds an element of this the Corporate and Legal Services department will send the request through to the Subject Access Team so that the request can be processed in accordance with subject access timelines. It will not be necessary for the applicant to submit an additional request.

<table>
<tr><td rowspan="2">Once the department responsible for collating the information for the FOI Request comes back, Corporate and Legal Services formulate and send out a response to the requester.</td><td>Does the information requested exceed the appropriate limit (18 hours work)?</td><td>Inform the requestor and offer assistance to reduce the work time required.</td></tr>
<tr><td>Does an exemption apply?</td><td>If yes, Corporate and Legal Services inform the requestor of the exemption</td></tr>
<tr><td colspan="3">Corporate and Legal Services update the FOI request Log.
Complete the date the Department replied
Complete date of response sent to the requestor (this should be within the 20 working days from receipt of request)
Save a hard copy of the request and save all documentation regarding the FOI on the intranet site in a folder marked with the Requestor’s name.</td></tr>
</table>

Appendix 23

Disposal of Information/Records

Information should only be disposed of where:

- there is no longer a requirement to retain it under the retention schedule
- it is a duplicate copy and the original record is still accessible and available if required
- it is a paper copy which has been scanned and stored electronically on the appropriate clinical system.

Consideration should be given to retention in relation to the national Goddard and other national Inquiries that include historical investigations and whether records should be retained for longer than the required retention period. For retention periods see (See Appendix 30).

Non-confidential paper-based information should be disposed of using the appropriate recycling facilities provided throughout Trust premises.

Paper-based information	Healthcare Records	Electronic Files
Use the confidential waste sacks or bins provided (through a contract with approved companies) or shred the document using a shredder that meets the required specifications for destruction of confidential NHS material (obtained through procurement).	The Senior Records Management Advisor must arrange for disposal of all healthcare records once they no longer need to be retained. Destruction will be authorised using approved contractors only.	Should be deleted from both the PC and the Trust network as necessary. All computer equipment that is no longer required must be returned to the IT department. Where equipment is to be re-allocated to a different staff member the line manager should seek IT advice before approving.

The Team Leader – Information Governance, Records and Privacy is responsible for developing a selection policy to identify which records are likely to be suitable for permanent preservation. These records will be moved into permanent preservation with Lincolnshire Archives.

The Team Leader – Information Governance, Records and Privacy will establish procedures for the closure of records when no longer current, the secure storage of archived records, and effective disposal, as soon as appropriate. Archiving arrangements should be reviewed to ensure value for money and Statutory obligations are met by approved contractor.

Destruction certificates for old records which have been destroyed and master copies of old CD ROMs will be stored with the Records Management Team.

Annual checks of records previously placed on CD ROM will be made to ensure that destruction of the CD ROMs (or earlier microfiche records) is carried out after the appropriate timescale.

The Senior Records Management Advisor will liaise with the archive company to authorise safe and secure destruction.

Certain records will be identified as “Not for Destruction”

- Record sets of major reports and publications and of the minutes of the Trust and its predecessors, together with those of major committees and sub committees should be selected for permanent preservation.
- Records which seem likely to provide material for research should be scrutinised with a view to permanent preservation, particularly those relating to:
    - The history of the Trust (including that of its predecessors) its organisations and procedures
    - The history of individual hospitals under the control of the Trust including matters relating to their history before the NHS and under predecessor authorities
    - Notable events or persons where the records add significantly to what is already known
    - Major events (whether in national, or purely local terms) or trends in political, social and economic events
    - Scientific, technological and medical research and development
    - Major plans and projects, including projects which have been abandoned or deferred
    - Industrial relations (not routine staff matters)
    - Records of benefactors in addition to those included in records of non-Exchequer funds
    - One set of the annual accounts and statements submitted to the Secretary of State for each year in accordance with the requirements of the National Health Service Acts; documents relating to the terms of any Trusts administered by the Trust whether or not they are included in records of non-Exchequer funds; key records, in addition to final accounts, relating to building and engineering works such as surveys, site plans, drawings, bills of quantities, contract documents, including those relating to major projects which have been abandoned or deferred.
    - Records which are evidence of title of property must never be destroyed. If documents of title have been lost, the administrative files relating to the ownership of land must be retained for as long as the documents of title would have been kept.

The Trust lodges historical information with the Lincolnshire Archives and access to the records is directed through the Archives to the Team Leader – Information Governance, Records and Privacy.

Appendix 24

Information/Records Audits

On an annual basis the Trust will undertake an audit of clinical coding data quality in accordance with Clinical Classification Service standards to enable compliance with the Data Security Protection Toolkit. The audit is part of the annual audit programme and will be undertaken by the Trust external auditors on 50 sets of clinical records. This ensures compliance with Data Security Protection Toolkit.

The Trust will undertake an inventory of all Trust records, both health and corporate records held in either hard copy or electronic formats. This is to ensure that all record collections/information sets are identified along with the volume of records held, the type of media on which they are held, their physical condition, their location, the environmental conditions in which they are stored and the responsible manager.

Audits of Trust premises will be conducted by the Compliance Team, with the aid of volunteers, who may be service users, carers or involved members of the Foundation Trust. This will examine the range of information leaflets etc. available at units, how up to date this information is and how the information is displayed.

The Informatics team will undertake both routine audits and targeted audits on specific requests from managers to examine access undertaken by staff to electronic records, clinical activity and any deletions or amendments made to clinical records. This audit activity enables the Trust to ensure confidentiality of information held and to reinforce security of access controls. Any concerns highlighted by this audit will be brought to the attention of the appropriate service manager for investigation.

The Trust Information Governance and Records Management Group will act as sponsors for the annual record keeping audit programme, which covers all services in the Trust. Every team will be expected to audit annually. They will audit records from all teams and services as part of an annual inspection which will also cover safeguarding, mental health act, care planning and deprivation of liberty.

Audit will be undertaken using the approved audit tools under Trust wide audit which are reviewed and approved by the Information Governance and Records Management Group on an annual basis. The minimum criteria for audit measurements include timeliness of entries, accuracy, attributability of entries, legibility and quality of clinical information on which decisions about service user care are based. An audit return will be based upon checking up to 10 sets of healthcare records per service against the above criteria.

On completion of the audit the Team Leader – Information Governance, Records and Privacy will share the completed audit tool with the manager of the service audited to enable local creation of action plans for improvement.

Teams will be required to supply evidence of the action plan completion for sign off at Information Governance and Records Management Group. Exceptions will be reported to the group for service nominated representatives to take back to their teams and ensure compliance with the audit programme is met.

An aggregated audit summary report will be produced by the Team Leader – Information Governance, Records and Privacy to summarise the results of each audit cycle.

The Audit report will be shared with the Information Governance and Records Management Group for areas of concern to be discussed, resolutions agreed and good practice recognised. Areas which require reporting to IM&T Committee will be identified by the Information Governance and Records Management Group and included in the Team Leader – Information Governance, Records and Privacy's report to IM&T Committee for ratification.

The Trust will complete a review of all records to check records retained in each service area, where they are held. This includes security arrangements, business critical assets, business continuity arrangements and identification of Information Asset Owners and Administrators, annually as part of the DSPT requirements.

Appendix 25

Provision of Leaflets to Service Users

It is the responsibility of all members of staff to alert their manager if they discover a need for information literature that is not being met. The manager will then produce a business case for developing an appropriate communication piece.

If a new leaflet is to be produced, or an existing leaflet amended, the author must see How do I produce a service leaflet on the Trust's intranet. Other staff, service user and carer groups and support groups should be consulted with, in drafting the text, where possible.

The first draft is submitted to the Communications Team who will check it includes all essential content. The Communications Team will set the leaflet in line with the Corporate style template.

The Communications Team and the author will recruit an appropriate reader's panel to assess the draft in terms of readability, comprehension and general appeal.

Once the leaflet has been approved by the service the Communications Team will liaise with the leaflet author about the format in which the information will be presented. If professional printing is required, the Communications Team will agree a print quantity with the leaflet author and source printing. A requisition will be raised by the Communications Team if the leaflet is to be funded corporately or by the leaflet author if it is to be funded by a local budget.

Photocopying of documents should be avoided where possible to ensure that the quality of the document is as high as possible. Where photocopying is unavoidable, the master copy of a document should be used to make all subsequent copies. Teams can contact the Communications Team on 01522 309191 or by emailing communicationslpft@lpft.nhs.uk for assistance and advice on this issue. The Communications Team will also be able to access the professional contracted company for large scale copying jobs.
The communications team will ensure that the leaflet is uploaded to the intranet or internet, dependent upon the audience type.

The Trust has a responsibility to ensure that all service users and other members of the public have access to information that can be easily translated or is available in a language they can understand. On request, the Communications Team can make leaflets available in large print, other languages, Braille and audio CD.

If a service user requests a leaflet in another language, the cost for this should be met by the team that is working with that service user. The Communications Team can offer guidance about translation agencies and information is also available on the Equality and Diversity site on SHARON.

All leaflets on the leaflet database will be given a review date of one year from its publication date. The Communications Team holds an electronic catalogue of all leaflets, their authors and publication dates, and will endeavour to make contact with each leaflet author once a year to prompt them to review their leaflet/s.

When a leaflet is no longer relevant or needed, the leaflet author will inform the Communications Team that it is to be taken out of circulation and give reasons why. The Communications Team will include a notice in the weekly word email and on the intranet informing staff that this leaflet is to be taken out of circulation and request that any stocks they have be removed and no longer used. The Communications Team will update the leaflet catalogue and database accordingly by moving the leaflet to the obsolete section of the leaflet archive and recording the reasons for removal. When a leaflet becomes obsolete, it will also form part of the Communications Team's quarterly update to the Involvement and Engagement Committee.

Appendix 26

Definitions

Appraisal – The process of evaluating an organisation's activities to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of Government accountability and the expectations of researchers and other users of the records.

Caldicott Guardian – The strategic lead within the organisation for development of internal protocols governing the protection and use of patient – identifiable information by the staff of their organisation and for agreements relating to cross boundary information sharing with partner organisations.

Clinical Coding – The diagnostic coding of service user episodes of care, activity, treatment and processes in accordance with national standards as defined by the World Health Organisation International Classification of Diseases and Related Health Problems.

Clinical Governance – Ensuring NHS organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care.

Confidential information - All **Person Identifiable Data** is confidential. Information about the business function of the Trust, which could be commercially valuable, such as financial or contracting information is also confidential. This covers information, the disclosure of which would be likely to:

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

Consent – Express (Explicit) Consent which is expressed orally or in writing (except where the service user cannot write or speak, when other forms of communication may be sufficient)

Consent – Implied Consent
Some uses and disclosures of data, for instance, routine record keeping, consultation of records etc., in the course of the provision of care and treatment, or clinical audit are effectively conditions of care / treatment. Such uses and disclosures may be described as 'routine' in the sense that acceptance of treatment, or provision of service by the service user, will imply consent to the processing of data for a specified purpose such as medical. Implied consent cannot justify sharing between partner organisations for other purposes, express consent is required.

Corporate Records – Records other than health records that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and its employees.

Current records – Records necessary to conduct the current and ongoing business of an organisation.

Data integrity – the completeness and accurateness of the data

Destruction – The process of eliminating or deleting records beyond any possible reconstruction.

Disposal – The implementation of appraisal and review decisions for the management of records.

Encryption – to convert electronic data into a code to prevent unauthorised access or amendment. There are differing levels of encryption which offer different levels of security of data. In this document 'encrypted' refers to data that has been encrypted to the standards required by the Information Governance Statement of Compliance and associated Codes of Practice and approved by the Trust.

Exemption – Provisions within Data Protection Act and Freedom of Information Act which define particular types of information which public authorities are not obliged to disclose.

Finished Consultant Episode – Defined by the NHS Data Dictionary as "The time a service user spends in the continuous care of one consultant using hospital site or nursing home bed(s) of one healthcare provider or in the case of shared care, in the care of two or more consultants. Where the care is provided by two or more consultants within the same episode, one consultant will take overriding responsibility for the service user and only one consultant episode is recorded." This therefore includes all inpatient admissions including those for respite care. An episode finishes when either the service user is discharged or the responsibility for care passes between Consultants.

Healthcare Record – A single record with a unique identifier containing information relating to the health of a given service user who can be identified from that information and which has been recorded in connection with the care of that service user. This may comprise text, sound, image and/or paper.

Information Governance – ensures that service user information and data for which the Caldicott Guardian is responsible is reliable, accurate, held securely at all times and of good quality.

Information/Records Audit – Looks at the means by which an information survey will be carried out and what the survey is intended to capture. It helps an organisation to promote control over its records and information and provides valuable data for ensuring legislation, policies and standards are complied with, suitable processes are used and controls put in place to ensure the completeness, relevance, correctness and security of data.

Information Commissioner – The Information Commissioner enforces and oversees the Data Protection Act 2018 and the Freedom of Information Act 2000.

Information Sharing Protocols Documented rules and procedures for the disclosure and use of patient information, which specifically relates to security, confidentiality and data destruction, between two or more organisations or agencies.

NHS Care Records Service – The electronic patient information system being introduced which will connect all health services in a single, secure national system which will enable individual patient electronic record details to be accessed by authorised personnel at the appropriate level anywhere in England.

NHS Number - A unique 10 character number assigned to every individual registered with the NHS in England and Wales, used as the common identifier for service users.

Person Identifiable Data (PID) is any information that can identify a person. This includes service users, staff their families or friends. Key identifiable information includes:

- Individual's name, address, full post code, date of birth;
- pictures, photographs, videos, audio-tapes or other images of service users or staff;
- Anything else that may be used to identify an individual directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

It may be held on paper, floppy disc, pen drives, USB Sticks, CD, computer file or printout, e-mail, text message, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops, palmtops, mobile phones, pen drives and digital cameras.

Portable Computer Equipment is a broad term encompassing any equipment or removable storage devices which are designed to be integrated with computer systems or networks. The term therefore includes laptop computers/notebooks, tablet PCs, handheld personal digital assistants (PDAs), **removable storage devices** and mobile phones capable of accessing the internet (including **Smart Phones** and blackberries),

Publication Scheme – A publication scheme is required of all NHS organisations under the Freedom of Information Act. It details information which is available to the public and how it can be obtained and in what format.

Records – Information created, received, maintained as evidence by an organisation in pursuance of legal obligations, or in the transaction of business. An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees – including consultants, agency or casual staff.

Records Management – Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transaction in the form of records.

Redaction – The process of removing, withholding or hiding parts of a record due to either the application of a Freedom of Information Act exemption or a Data Protection Act Exemption.

Retention – The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their eventual disposal, according to their administrative, legal, financial and historical evaluation.

Sensitive Personal Data Means Personal Data consisting of information as to:

a.) the racial or ethnic origins of the data subject;
b.) his political opinions;
c.) his religious beliefs or other beliefs of a similar nature;
d.) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992;
e.) his physical or mental health or condition;
f.) his sexual life;
g.) the commission or alleged commission by him of any offence; or

h.) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in such proceedings.

SIRO - Senior Information Risk Owner The SIRO is a Board level Director who is responsible for owning the information risks of the Trust. The SIRO oversees the appropriate management of all information assets (produced in or belonging to the Trust) in the form of an information asset register which provides a focal point for managing all information risks and incidents. The SIRO acts as an advocate for information risk on the Trust Board.

Tracking – Creating, capturing and maintaining information about the movement and use of records.

Appendix 27

Duties

Further information on duties can be found in the Corporate Governance Document – Scheme of Delegation.

Individual/ Group	Responsible For:
Chief Executive	As Accounting Officer of the Trust the Chief Executive has ultimate responsibility for staff and organisational adherence to legislation, guidance and policy. Ensuring appropriate management chains are in place to enable adherence to this policy.
Board of Directors and Board Sub-Committees.	Ensuring that the Trust has in place the necessary policies and procedures to enable staff to meet the standards aimed at by the Trust. Allocating resources required for implementation of policy. Receiving reports and approving action plans as detailed at section 12.
Caldicott Guardian	The Medical Director is the Caldicott Guardian for the Trust and has particular responsibility for reflecting service users' interests regarding the use of person identifiable information ensuring that Caldicott Principles are embedded in the Trust. Board Lead for risk management, thus ensuring risks associated with information systems are monitored and addressed.
Director of Finance	Senior Information Risk Owner (SIRO). Data Protection Lead. Registered with the ICO. Ensure that the Trust has robust policies and procedures in place to ensure the security of information held and communicated. To ensure the contracts with organisations providing ICT services are robust and monitored. To ensure the contracts with organisations providing Electronic patient records are robust and monitored. Director lead for information management. To ensure the Board is fully briefed on areas of responsibility and Executive Committee decisions. Director lead for records management
Information Management and Technology Committee	Approve the policy. Monitor all aspects of policy Receiving reports and approving action plans as detailed at Appendix 28.
Information Governance and Records Management Group	Monitor relevant Information Governance and Records Management aspects of the policy and elevate areas of concern and action plans to the IM&T Committee for ratification.
Data Quality Assurance and Steering Group	Monitor relevant Data Standards, Information Management and Clinical Coding aspects of the policy and elevate areas of concern and action plans to the IM&T Committee for ratification.

Team Leader - Information Governance, Records and Privacy	Responsible for the overall development of records management and information governance strategy and policy ensuring compliance with legislation, national standards and requirements. Gather evidence from audits to present to the appropriate parent group to monitor compliance with standards and inform future policy development and training requirements and enable formal reporting to the Board of Directors for areas of risk. Responding to requests for access to patient information within the statutory time limits. Manages the Subject Access Team. Nominated as Data Protection Officer for the Trust in accordance with GDPR requirements. Provide advice and support to senior managers on all aspects of records management and information governance.
Deputy Director of Informatics	Responsible for the overall development of information governance strategy and policy ensuring compliance with legislation, national standards and requirements. Acts as Security Information Manager for the Trust to ensure the security and integrity of systems owned and operated by the Trust. Gather evidence from audits to present to the appropriate parent group to monitor compliance with standards and inform future policy development and training requirements and enable formal reporting to the Board of Directors for areas of risk.
Informatics Team	Responsible for the overall development of information management and data quality policy ensuring compliance with legislation, national standards and requirements. Gather evidence from audits to present to the appropriate parent group to monitor compliance with standards and inform future policy development and training requirements and enable formal reporting to the Board of Directors for areas of risk. Interpret the reporting requirements of the Trust Liaising with EIS managers/administrators to ensure each system will capture the required information Monitor and disseminate all changes to reporting requirements (e.g. DSCNs)
Human Resources Department	Provide timely updates of leavers to ICT to allow disabling of their access from the Trust network. To ensure a confidentiality clause is included in all contracts of employment. To support any investigations regarding breaches of this policy. To assist line managers in ensuring the appropriate reference is made to responsibility for information in role profiles..
Corporate and Corporate and Legal Services Team	Providing advice to staff on the legal issues which may arise from the implementation of this policy. Responding to Freedom of Information requests within the statutory time limits.

Communications and Marketing Team	Ensuring the most appropriate means to communicate the proper application of this policy throughout the Trust. Assisting members of staff with written forms of information. Ensuring that information is in the corporate style in terms of content and layout/design. Assisting teams in finding appropriate service users to feedback on Trust leaflets in relation to language and readability, prior to prnting and publication. Scoring appropriate details of members of the previous Readers Panel in accordance with the Data Protection Act 2018. Advising on getting information produced in different formats e.g. alternative language, large print or Braille. Advising on professional print services and acting as a point of contact between printers and staff, if any problems or queries arise. Advising on the funding of leaflets (leaflets are normally funded from the corporate budget if they involve county-wide service. Local information may be required to be funded through local budgets). Maintaining the archive of leaflets which is to include hard copy and electronic versions of leaflets.
Membership and Engagement Team	Storing the personal details of members of the Foundation Trust in accordance with the Data Protection Act 2018.
Learning and Development Department	Ensuring appropriate and sufficient training is available and promoted to give staff the knowledge and skills to comply with this policy. Ensure delivery of Mandatory training to cover induction for all new staff and Records Management and Information Governance modules on an annual refresher basis. Ensuring information on training is easily accessible to staff. Develop and implement training needs analysis to assess, train and develop needs of staff, consideration of how needs can be met and evaluation of training undertaken. Ensuring a training database is maintained of each staff member's attendance at training Providing reports on the uptake of training as per the requirements at section 12.
Information Asset Owners	IAOs are senior individuals with responsibility for one or more information assets. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. Participates in the annual data flow mapping process to ensure that the Trust can manage and mitigate and risks in respect of information being used/received by the organisation.
Information Asset Administrators	IAAs administer the above assets on a daily basis and provide evidence and assurance to the owners to enable assurance that the Trust is meeting its regulatory requirements.

General Managers/Clinical Directors/ Lead Specialists/ Heads of Service	Ensuring staff are familiar with this policy (including volunteers, placement staff, students, temporary staff and contracted staff) Ensuring staff have the tools, resources and skills to deliver the standards detailed in this policy and to undertake the tasks requested of them. Assessing training needs of support staff according to job role and level of access to person identifiable information and responsibilities for processing and managing records. Ensuring all efforts are made to facilitate staff attendance at mandatory training and formal induction training as defined in the HR Policy Handbook. Ensuring all staff newly appointed to the Trust receive local induction on their specific responsibilities for Information Governance and how this affects their day to day working practice. Ensuring relevant legislation, Codes of Practice and guidance are available to staff. Gathering assurance that requirements and standards are being met and providing reports to the SIRO as detailed at section 12 and as required. Ensure that access to Trust systems are enabled/amended/disabled when staff start/change roles/leave employment to maintain system security.
All Staff	Practicing within the legislative framework and update knowledge of such accordingly. Complying with professional Codes of Practice relevant to their discipline. Following the procedures described in this policy and aim to achieve the target standards. All staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate, legible records of their work in the Trust and manage those records in keeping with this policy. All Trust staff where appropriate must make entries into healthcare records in respect of any contact with the service user or about the service user in accordance with the procedure outlined at section 5.3.3 and 5.3.4 of this policy. Staff are only entitled to access the records for patients with whom they have a legitimate professional working relationship through LPFT. All staff must ensure that the service user demographic details are checked with the service user and updated regularly to ensure that the record is accurate and up to date and meets the requirements of the Data Protection Act 2018 and data standards requirements. Undertaking all mandatory training as identified in HR Policy Handbook and any training essential for their particular role or duties. Information Governance and Records Management training is mandatory annual training for all disciplines. Cooperating with management to meet requirements Providing reports to General Managers/Clinical Directors on the performance against standards for their team.

Appendix 28

Monitoring Arrangements

Standard	Measurables	Lead	Frequency	Reporting to	Action Plan/ Monitoring
All mobile computing equipment and mobile telephone devices are encrypted to the required standards and used appropriately	No. of incidents involving mobile computing equipment.	Head of Informatics Report from Datix	Bi-monthly Monthly	IM&T Committee IG/RM Group	Action Plan: IG/RM Group Monitoring: IM&T
To ensure all Freedom of Information requests are managed appropriately	Reports detailing exceptions and breaches through benchmarking.	C&LS Manager	Bi- Monthly	IM&T Committee	Action Plan: C&LS Manager Monitoring: IM&T Committee
Contracts/MOUs in place for all external visitors who will have access to information held by the Trust to ensure they comply with this policy.	Audit of contracts	Team Leader Records, IG and Privacy	Annual	IG/RM Group	Action plan as part of annual Data Security Protection Toolkit submission
All documents scanned by the Trust (in order to destroy the original) have the maximum evidential weight reasonably achievable.	Risk assessments accompanying departmental procedures Results of audits of departmental processes	Department Head IG/RM Group	As required	IM&T	Monitoring: IM&T
Staff use of the email service is appropriate and maintains	No. of incidents where email used inappropriately	Department Heads Report from Datix	Monthly	IG/RM Group	Action Plan: IG/RM Group Monitoring:

Standard	Measurables	Lead	Frequency	Reporting to	Action Plan/ Monitoring
network security as well as confidentiality					IM&T
Systems in place to monitor the number of confidentiality breaches and security incidents	No. of information security breaches and associated root cause	Report from Datix Team Leader – Records Management, IG and Privacy	Monthly	IG/RM Group	Action Plan: IG/RM Group Monitoring: IM&T
To achieve compliance with Data Security Protection Toolkit assertions.	Report following audit assessment	Team Leader – Records Management, IG and Privacy	Annually	IM&T	Action Plan: IG/RM Group Monitoring: IM&T
All Subject access requests facilitated within required timescale.	Reports detailing exceptions and breaches through benchmarking.	Team Leader – Records Management, IG and Privacy & Head of HR	Monthly	IG/RM Group, exception reporting to IM&T	Action Plan: Team Leader – IG/RM and Privacy Monitoring: IG/RM IM&T
Systems in place to monitor the occurrence of missing records	Number of incidents of missing records	Datix report and IG/RM group	Bi monthly	IM&T	Action Plan: IG/RM Group Monitoring: IG/RM Group and IM&T
Systems in place to monitor the standard of record keeping	Records audit Achievement against local action plan following audit	Team Leader - Information Governance, Records and Privacy	Annually – full report	IM&T	Action Plan: IG/RM Group & Team Leaders Monitoring: IM&T
All staff who create or maintain records have	Number of staff attending training broken down by division and staff	Learning and Development Department	Monthly	Divisional business managers and	Action Plan: Learning & Developme

Standard	Measurables	Lead	Frequency	Reporting to	Action Plan/ Monitoring
received appropriate training	group through Service Line reporting.			Corporate Managers	nt Department / Team Leader – IG/RM and Privacy and Service Leads Monitoring: IM&T
Systems in place to ensure records are archived and destroyed appropriately	Number of records culled from main collections and sent to archive Number of records destroyed and certificate of destruction obtained	IG/RM Group	Quarterly	IM&T	Action Plan IG/RM Group Monitoring IM&T
To maintain high standards of data quality including clinical coding.	Number or data quality issues reported to/ identified by the Information department (through standard error/missing data reports). Number of changes as a result of DSCNs Audit of data quality – check run against specified data item within the Electronic patient records Monthly report on clinical coding following discharge/transfer (FCEs) - % coded and un-coded	Informatics Team leader, Performance Support Officer and Data Quality Group Informatics Team Leader Informatics Team Leader Performance Team	Monthly Monthly/Quarterly Quarterly (internal)	IM&T Operational Directorate Meeting/ IM&T	Action Plan: Data Quality Group Monitoring: IM&T

Standard	Measurables	Lead	Frequency	Reporting to	Action Plan/ Monitoring
	Audit of clinical coding against records for FCEs	Performance Team	Annually (Connecting for Health)	IM&T	
Systems in place to monitor the process for the development of service user information, including essential content, review process and review date	Number of new leaflet requests per year Number of new approved leaflets per year Number of leaflets assessed against essential content list Number of reviewed leaflets approved Number of reviewed leaflets withdrawn Number of leaflets due for review in year	Communications Team	Quarterly Report Annual Audit	Strategy, performance & information directorate meetings	Report Strategy and Performance and Information Directorate Meeting
Systems in place to monitor archiving of leaflets arrangements	Number of active leaflets held on leaflet database approved for use Number of inactive leaflets held on database as obsolete Number of leaflets under development.	Communications Team	Quarterly Report Annual Audit	Strategy, performance & information directorate meetings	NHSLA compliance Internal audit

Appendix 29

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

2018/2019

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	IG Lead	Director of Finance (SIRO)/Deputy Director of Informatics
	Senior Information Risk Owner (SIRO)	SIRO Director of Finance and Information (SIRO)
	Caldicott Guardian	Medical Director
	Registration Authority	Trust's IT Provider
	Information Security	Deputy Director of Informatics
		Team Leader Information Governance, Records and Privacy
	Freedom of Information	Trust Secretaries Office
	Information Governance and Records Management and Data Protection	Team Leader Information Governance, Records and Privacy
	Data Protection Officer (Data Protection Act 2018 & GDPR requirement)	Team Leader Information Governance, Records and Privacy
Key Policies	Records Lifecycle Management and Information Governance Policy 8a Information Management and Security Policy 8b ICT Systems Use Policy 8c Records Management and Information Lifecycle Strategy Lincolnshire Inter-Agency Information Sharing Protocol 8d IM&T Strategy	The policies are all held on the Trust Internet and are reviewed on an annual basis and signed off by the appropriate governance group with responsibility and then taken to Information Management and Technology Committee for final ratification.

Key Governance Bodies	Information Governance and Records Management Group Data Quality Group Programme Delivery Group	Collectively these groups have responsibility for the Information Governance agenda and All groups report through to the Trust IM&T Committee. Each group has a ratified terms of reference, minutes and papers for each group are held on the Trust Intranet. IM&T Committee reports through to Finance and Performance Committee which is a sub group of Board.
Resources	Senior Information Risk Owner	The Director Lead for Information Governance (SIRO) will hold the budget for internal IG as part of their role as budget holder for Lincolnshire Partnership NHS Foundation Trust and will be responsible for highlighting any resourcing issues and improvements required either in year or for the forthcoming year.
Information Governance Framework	Details of how responsibility and accountability for IG is cascaded through the organisation.	Provisions for IG are contained in all staff contracts, contracts with volunteers and honorary contracts and agency staff. Contracts with third parties similarly contain provision for IG clauses. Information Asset owners and Information Asset administrators are identified throughout the organisation and have been identified through completion of data flow mapping and information asset registers. All third party contractors are checked for DSPT compliance. Services are briefed on IG matters through service representation at appropriate governance group meeting; there are regular briefings through communication channels and lessons learned bulletins. All staff are mandated to attend annual refresh IG training.
Training & Guidance	Staff Code of Conduct Training for all staff (see Key Policies) Training for specialist IG roles	All Staff receive a copy of the code of conduct on induction and are also furnished with the staff handbook. Staff are informed of their responsibilities as part of induction and the consequences of failing to follow policies and procedures. All policies and procedures are available through a link on desk tops to the Trust website for all policies. It is mandated that all staff receive training appropriate to their roles in respect of IG and this is done through induction training and bespoke training in the workplace. IG training is mandated for annual refresh. Specialised roles for IG receive annual training appropriate to their roles in order to uphold current knowledge and expertise.
Incident Management	Documented procedures and staff awareness through the Reporting and Management of Risk Policy(Policy 5b)	Clear guidance on incident management procedures are documented in the policy and staff should are made aware of its existence at induction and refresh training. All incidents are reported through the Datix incident reporting system and are reviewed by the appropriate governance group to identify issues for escalation, commission investigations and apply lessons learned, identify trends.

1. Introduction & Purpose

The Information Governance Framework brings together related initiatives concerned with improving the security, processing, quality and handling of information. It Incorporates the Data Protection Act 2018, the Freedom of Information Act 2000, the Human Rights Act 1998 and the common law duty of confidence. It also incorporates the NHS Code of Confidentiality; Information Security Assurance, Information Quality Assurance and Records Management and underpins the NHS Care Record Guarantee.

2. Scope

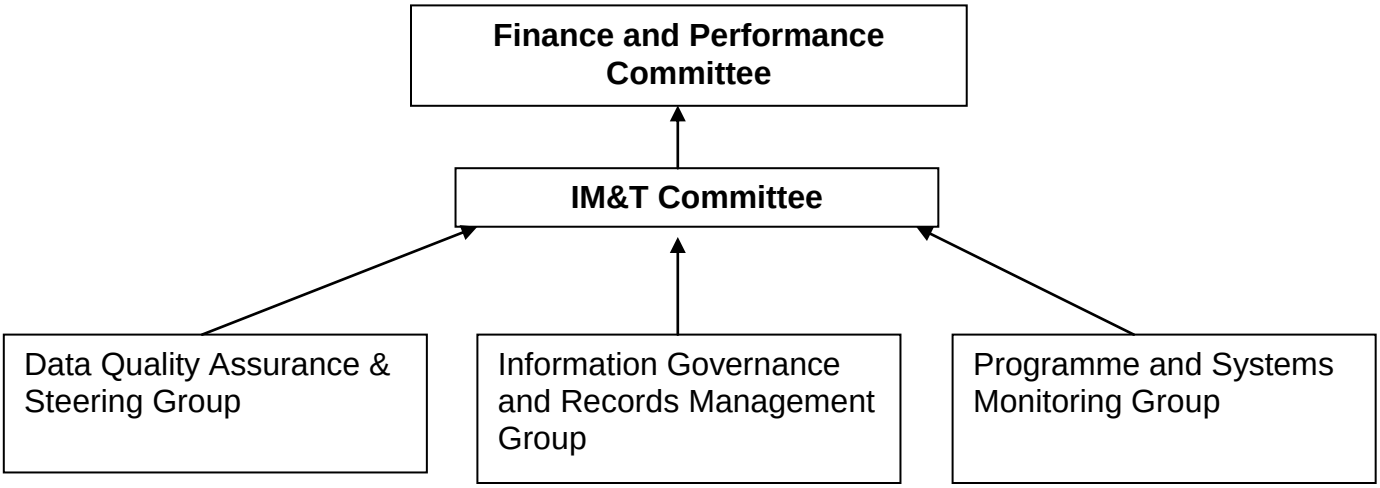
The IG Framework is the control assurance framework which is formed by those elements of law and policy from which applicable Information Governance standards are derived. It applies only to internal Information Governance assurance.

3. Policy

All policies will be disseminated/cascaded via Lincolnshire Partnership NHS Foundation Trust Communication Team. Lincolnshire Partnership NHS Foundation Trust IG Lead will attend the IM&T Committee in order to brief respective leads to ensure a robust cascade of information.

To obtain assurance that implementation of policies and the development of robust information governance is subject to effective planning, Lincolnshire Partnership NHS Foundation Trust IG Lead will utilise and review audit and incident findings that are IG related and report these to the IM&T Committee through the Information Governance and Records Management Group highlight report. This information will also form part of the awareness campaign for IG with serious incidents forming part of the Information Governance and Records Management Group and IM&T Committee Risk Register.

4. Internal IG Governance (Bodies & Structure)



5. IG Awareness

To ensure that raising awareness of a compliance with information governance standards is raised. Lincolnshire Partnership NHS Foundation Trust will utilise locally produced codes of conduct for security and confidentiality further supported by the leaflet from the department for health on Confidentiality and Information Sharing for Direct Care.

To ensure that this campaign has been implemented and all staff have been informed of their responsibilities a staff survey will be undertaken as part of IG site audits to test understanding of Information Governance standards.

In addition it will continue to raise awareness about national and local incidents that require cascading by doing this through identified communication routes and highlighting trends of incidents and actions required through the lessons learned bulletins.

6. IG Internal Reporting

Lincolnshire Partnership NHS Foundation Trust Board of Directors receive periodic assurance that management and accountability for IG arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by IG updates within the IM&T Committee report.

The IG Work stream is included within the Information Governance and Records Management Group Work Plan and will also:

- Report IG incidents to the Information Governance and Records Management Group
- Analyse, investigate and upward report of incidents and any recommendations for remedial action

- Produce IG work programme progress reports
- Report on annual IG assessment and improvement plans
- Communicate IG developments and standards to appropriate forum and staff
- Brief SIRO on information management and risk to ensure that Trust Board is adequately briefed and assured

Policy and procedures for actual and potential breaches of confidential and person identifiable information are aligned with the guidance provided within the 'Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents' and Data Protection Act 2018 requirements with regards reporting to the ICO.

7. Caldicott Function

Lincolnshire Partnership NHS Foundation Trust must have in place a recognised senior level Caldicott guardian. The Caldicott functions will be maintained by the Caldicott Guardian supported by the Team Leader for Records Management, Information Governance and Privacy and with further support from the Records Management and Information Governance Group.

Any issues, incidents and strategy relating to this function will be incorporated within overarching internal Information Governance arrangements.

8. Data Security Protection Toolkit and independent auditing

The Trust will complete the requirements of the self-assessment against the standards in the Data Security Protection Toolkit and submit them periodically as required. The Trust will also undergo an annual independent audit of its IG arrangements and its clinical coding arrangements and processes. The findings will form part of the overall IG and Caldicott Guardian work plan.

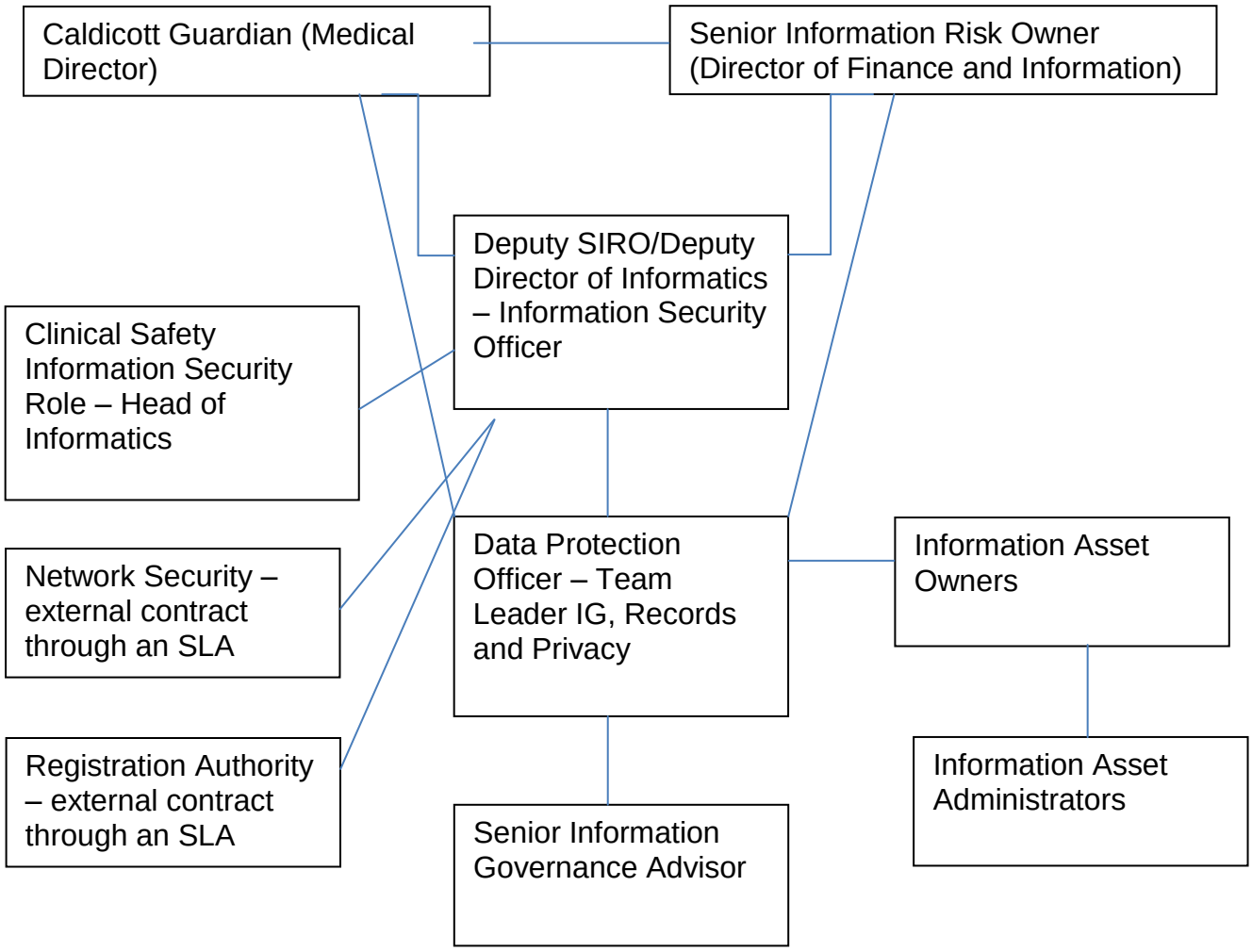
In addition the Trust will complete audits of its systems and processes at least on an annual basis including:

- Review of data flow mapping.
- Review of its network and server security
- Review of its critical information systems management and access controls

9. Review of this Framework

These arrangements and the framework document will be reviewed at least annually.

LPFT INFORMATION GOVERNANCE MANAGEMENT STRUCTURE



Appendix 30

LPFT Records Retention Schedule
Information Extracted from Records Management Code of Practice July 2016

RECORD TYPE **Healthcare Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Supporting Clinical Documents		
Audio tapes of calls requesting care i.e. Crisis teams or Single Point of Access	1 year from creation	Destroy
Clinical audit records	5 years	Destroy
Clinical trials master files of a trial authorised under the European portal under regulation (EU) No 536/2014	25 years after closure of trial	Transfer to Lincolnshire Archives
Research dataset	20 years on closure of research	Transfer to Lincolnshire Archives
Research ethics committee documentation for research proposal	Termination of research plus 5 years	Transfer to Lincolnshire Archives
Research ethics committee minutes and papers	20 years from year to which they relate	Transfer to Lincolnshire Archives Destroy
Clinical trials of medicines – master file (file of a trial authorised under European portal)	25 years after closure of trial	
Research governance paper for individual studies	3 years after closure of study	
Court reports	8 years	Destroy
Discharge books (where they exist in paper format)	8 years after the last entry	Transfer to place of deposit

RECORD TYPE **Healthcare Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Handover Sheets	2 years	Local agreement following risk review recommendation
Observation Sheets	2 years	Locally determined retention date agreed at records management
Patient's property books/registers (property handed in for safe-keeping) including financial information e.g. patient monies	6 years after the end of the financial year in which the property was disposed of or 6 years after the register was closed.	Destroy
Record of custody and transfer of keys	2 years after last entry	Destroy
Referral letter for patients referred to health or care services but not accepted	2 years.	Destroy
Any reference to conclusion of treatment in the following recommended minimum retention periods, should be taken to include all follow-up checks and action in connection with the treatment		**The retention periods indicated apply to health and social care records in whatever medium they exist, i.e. manual, CD Rom, Microfiche, scanned electronic information.**
Assessment Folders – healthcare folders (green) which contain initial assessment details only	8 years	Destroy
Chaplaincy Records	2 years	Destroy

RECORD TYPE **Healthcare Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Child and Adolescent Including Youth Offending Service	Retain until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment, whichever is the longer period. Retention period for records of deceased persons is 8 years after death. If the illness could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain the records for a longer period.	Destroy
DART records	Treat as though mental health record (20 years)	Destroy
Electronic Patient Records System (EPR)	See notes	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.
GP Patient Records	Life of the patient + 10 years	Destroy

RECORD TYPE **Healthcare Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Learning Disabilities	Retain for the period of time appropriate to the patient/ speciality, e.g. children's records should be retained as per the retention period for the records of child and adolescent: mentally disordered persons (within the meaning of the Mental Health Act 1983) 20 years after the last entry in the record **or** 8 years after the patient's death if patient died whilst in the care of the organisation.	Destroy
Looked After Children (records that are NHS records that belong to clinical staff but which are held by the parent)	At the end of an episode of care the NHS organisation responsible for delivering that care and compiling the record of the care must make appropriate arrangements to retrieve parent-held records. The records should then be retained until the patient's 25th birthday or 26th birthday if the young person was 17 at the conclusion of treatment, or 8 years after death.	For patients who are 18+ and still receiving treatment their records should either move into adult services on transition or if they remain with LAC services should be treated as an adult record and retained for 20 years.
Mental Health Records The Trust has made the decision that all adult mental health records regardless of the discipline i.e. Mental Health, IAPT, DART, LD will be retained for 20 years	20 years after date of last contact between the service user and any healthcare professional employed by the Trust. 8 years after the patient has died from natural causes, 10 years if it is an untoward death	When the records come to an end of their retention period they must be reviewed to take into account any genetic implications of the service user's illness. Further retention should be subject to regular review.
Prison healthcare records	Where hospital letters for serving prisoners are scanned into the Prison Health computer system and the paper copy is also filed into the paper records the paper copy may be destroyed once it has been scanned into the system providing the scanning process and procedures are compliant with BSI's "BIP:0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically". Once the letters have been scanned they can be destroyed under confidential conditions	The paper record transfers with the prisoner to any new prison establishment. For records which remain the property of LPFT the record should be retained for 20 years following prisoner discharge from treatment or transfer to new provider.

RECORD TYPE **Healthcare Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Patient Activity Data	3 years	
Secure Unit Records	Classed as mental health records and can be retained for longer periods of time – normally in excess of 30 years for continuity of care	Review on case by case basis for public interest test – move to archive deposit
Private Patients	Although technically exempt from public records Acts it would be appropriate for Trusts to treat such records as if they were not exempt.	Retain for same period as mental health records
Scanned records	Retain for the period appropriate to the specialty as identified elsewhere in this schedule. Providing the scanning process and procedures are compliant with BSI's "BIP:0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically". Once the letters have been scanned onto the relevant electronic system the paper records can be destroyed under confidential conditions	
Staff wellbeing service "patient" records	12 years from date of discharge	Locally determined retention period
Video Records/voice recordings relating to patient care, video records/video conferencing relating to patient care, DVD records relating to patient care	Keep for the life of the patient record as per other retention periods in this schedule unless there has been local agreement made with the patient in respect of recordings i.e. when they are solely for use in training/study rather than for care purposes	Destroy
X-ray images and reports	To be considered as a permanent part of the patient record	

Please note that destruction of all records should take place in confidential conditions to ensure that information is disposed of safely and securely and in keeping with legislative requirements. For advice please contact your local healthcare records library or the Trust Records Manager.

RECORD TYPE Corporate Records	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Financial Records		
Accounts – Final Annual Accounts Report	Before 20 years	Deposit in Lincolnshire Archives
Accounts – all associated documentation and records for the purpose of audit as agreed by the auditors	3 years from end of financial year	Destroy
Financial Records of Transactions	6 years from end of financial year	Destroy
Debtor records cleared	2 years from close of financial year	Destroy
Debtors records not cleared Donations	6 years from close of financial year	Destroy
Petty Cash	2 years from end of financial year	Destroy
Benefactions	8 years after end of financial year in which Trust monies become finally spent or the gift in kind is accepted.	These may already be in the financial accounts and may be captured in other records/reports or committee papers. For benefactions, endowment. Trust fund/legacies, offer to a Place of Deposit.
Salaries paid to staff	10 years from close of financial year	Destroy
Staff Expense claims including travel and subsistence	6 years after end of financial year	Destroy
Superannuation records	10 years from close of financial year	Destroy
VAT records	6 years after the financial year they relate to	Destroy
Estates Records (including Health and Safety)		

RECORD TYPE **Corporate Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Accident Books/Records Health and Safety Documents	3 years	Destroy
Building plans and records of major building work	Lifetime of building or disposal of asset plus 6 years	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit/
Inspection reports	Lifetime of installation	Review and destroy
Close Circuit TV images (CCTV)	31 days (unless images have been identified as evidence for an investigation/serious incident then they should be downloaded and retained along with all other information for the incident investigation process)	Erase permanently
Deeds of Title	Retain while the organisation has ownership and then pass on with sale of property. If Land Registry certificate exists, place deeds in Lincolnshire archive.	
Equipment monitoring and testing, inspection and maintenance work Employee Exposure monitoring information	10 years after equipment decommissioned 40 years for identifiable employees or 5 years for general information	Destroy Destroy
Fraud case files	6 years	
Leases	Termination of the lease plus 12 years	Destroy
Minor Building works	Completion of work retain for 6 years	Destroy
Procurement		

RECORD TYPE **Corporate Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Contracts – financial approval files Contracts – financial approved suppliers documentation Contracts sealed or unsealed	15 years on termination of contract 11 years when supplier finishes work 6 years on termination	Destroy
Tenders successful and unsuccessful	6 years from award date	Destroy
Stores records – major	6 years	Destroy
Stores records – minor (requisitions, issue notes, transfer vouchers, goods received etc.) Supplies records – minor (invitations to tender and inadmissible ledgers, routine papers relating to catering, furniture, equipment, stationery)	18 months 18 months	Destroy
Staff Records and Occupational Health		
Duty Rosters	6 years from end of financial year	Destroy
Flexi working hours (personal record of hours actually worked)	6 months	
CV's for non-executive directors (successful)	5 years following term of office	
CV's for non-executive directors (unsuccessful)	2 years	

RECORD TYPE **Corporate Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Human Resources Records (Personal files, staff training records) including care and non-care roles, evidence of right to work, security checks and recruitment documentation, contracts, references and related correspondence), occupational health reports ▪ this should include medical staff records and agency locum staff	6 years for full record and then create a summary to be retained until 75th birthday	Destroy
Job advertisements Job descriptions Job applications (unsuccessful)	1 year 3 years 1 year	
Staff training records	Records of significant training must be kept until 75th birthday or 6 years after staff leave **Clinical training** – 75th birthday or 6 years after staff leave **Mandatory training** – 10 years after training completed **Other training** – 6 years after training completed	
Supervision notes	3 years	
Superannuation Accounts and Registers and Copy Forms SD55 and SD55J	10 years original to NHS pensions agency	
Timesheets (for individual members of staff)	2 years after the year to which they relate	Destroy
FOI/SAR/Complaints/Risk		
Complaints case file	10 years from completion of incident	Destroy (Complaint information should never be held on the patient healthcare record

RECORD TYPE **Corporate Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Freedom of Information requests	3 years after full disclosure 6 years if there is an appeal	
Incidents (Serious level 2a and above) Incidents less serious including accidents	20 years 10 years	Transfer to Lincolnshire Archives Review and if no longer needed destroy
Industrial Relations (Not routine staff matters) including Industrial Tribunals	10 years from end of financial year	Destroy
Litigation dossiers	10 years on closure of case	
Receipt for registered, special delivery and recorded delivery mail	2 years following end of the financial year	
Subject Access requests and disclosure correspondence Subject Access cases where there has been an appeal	3 years 6 years	Destroy
Corporate Memory		
Board meetings, closed board meetings, committee listed in scheme of delegation or that report into the Board	Retain locally for up to 20 years and then transfer to Place of Deposit	Transfer to Lincolnshire Archives
Chief Executive records	This may include e-mails and correspondence where they are not already included in the board papers and they are considered to be of archival value	Transfer to Lincolnshire Archives
Destruction Certificate or Electronic metadata destruction stub or record of information held on destroyed physical media	20 years	Transfer to Lincolnshire Archives

RECORD TYPE Corporate Records	MINIMUM RETENTION PERIOD IN YEARS	NOTES
E-mail	Clinically relevant e-mail should be saved in full including any attachments into the patient electronic record the original e-mail can then be deleted from the system. Business relevant e-mail should be saved in the record keeping system according to the business to which it relates i.e. a SharePoint site relating to meetings/committees, project documents for a business change.	Once e-mail is securely saved in appropriate storage medium then the original e-mail can be deleted.
History of Organisation or predecessors (establishment order)	20 years	Transfer to Lincolnshire Archives
Intranet site	6 years	Transfer to Lincolnshire Archives
Meetings and minutes papers ((not listed in scheme of delegation) includes minor meetings/projects and departmental business meetings	6 years	Destroy
Patient advisory (PALS) records	10 years from end of financial year	Destroy
Patient Information Leaflets	6 years after the leaflet has been superseded	Transfer to Lincolnshire Archives
Patient surveys (regarding access to services etc.)	2 years	Destroy

RECORD TYPE **Corporate Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Policy, strategies and operating procedures	Lifetime of organisation + 6 years	Transfer to Lincolnshire Archives
Software licences	Lifetime of software	Destroy
Website	6 years	Transfer to Lincolnshire Archives
Miscellaneous		
Audit records and reports – originals	2 years from completion of audit	Destroy
Clinical diaries (information must be transferred to patient record)	2 years	Destroy
Corporate diaries	1 year	Destroy
Controlled drugs information	7 years from end of calendar year	Destroy
Non-clinical quality assurance records	12 years from end of year to which assurance relates	Destroy
Pharmacy Prescription records	2 years after the last treatment	Destroy
Phone message books/signing in books (any clinical information should be transferred to the patient record)	2 years	Destroy
Press cuttings Press releases and important internal communications	1 year 6 years	Transfer to Lincolnshire Archives
Project files (over £100,000)	6 years on termination of project, abandonment or deferral	
Project files (less than £100,000)	2 years on termination	

RECORD TYPE **Corporate Records**	MINIMUM RETENTION PERIOD IN YEARS	NOTES
Project Team files – summary only	3 years	
Public Consultations	5 years	Transfer to Lincolnshire Archives

Please note that destruction of all records should take place in confidential conditions to ensure that information is disposed of safely and securely and in keeping with legislative requirements. For advice please contact your local healthcare records library or the Trust Records Manager.