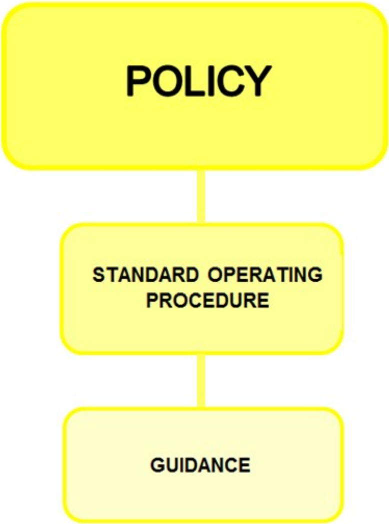
Lancashire Care NHS
NHS Foundation Trust

Corporate Records Management Policy

UNIQUE POLICY REFERENCE	IM&T 015
APPROVAL DATE	01/03/2017
REVIEW DATE	01/03/2019
POLICY AUTHOR	Information Governance, Assurance and Compliance Lead
ACCOUNTABLE DIRECTOR	Chief Finance Officer and Senior Information Risk Owner (SIRO)
APPROVED BY	Chief Finance Officer /SIRO

TRUST GOVERNANCE STRUCTURE
POLICY LINKED TO *Corporate Governance & Compliance Sub-Committee*



POLICY VERSION CONTROL

This record shall detail all previous versions of the Policy, including versions that have been known by other names and the date of when a new version was created.

Previous Versions (Title)	Date Reviewed	Why was a new version created?
Corporate Records Management Policy	*June 2015*	*Policy updated to take account of revised NHS Code of Practice for Records Management 2016 and Trust new Corporate Policy standard*

With acknowledgement to the IG Project Support Officer for their assistance with preparing this document.

1. TRUST POLICY STATEMENT

The Principle legislation governing the management of records is section 46 of the Freedom of Information Act 2000. The Act directs organisations to have record management systems which will help them perform their statutory duties.

All records created and maintained by the Trust are public records under the Public Records Act 1958 and 1967 and may be subject to both legal and professional obligations. The Trust will ensure that records management policies and procedures are in accordance with the following statutory and NHS guidelines:

- Data Protection Act 1998
- Freedom of Information Act 2000
- NHS Code of Confidentiality
- MNC Guidelines for Records and Record Keeping 2009
- NHSLA Risk Management standards for NHS Trusts
- Information Governance Toolkit (IGT) requirements (Req's 603 and 604)
- Monitor regulation
- NHS Records Retention Schedule
- Records Management Code of Practice for Health and Social Care

In addition staff associated with certain professional bodies must also adhere to their own professional codes of practice and conduct as part of their profession.

Corporate records management is the process whereby the Trust manages all aspects of Corporate records whether internally or externally generated and in any format or media type, from creation to disposal. Records are the Corporate memory, providing evidence of actions and decisions and representing a vital information asset to support daily functions and operations. Records must have the characteristics of authenticity, reliability, integrity and usability.

Definition of a Corporate Record and Types of Records
A Corporate Record is defined as information in any media which has been created or gathered as evidence of undertaking work activities in the conduct of its business. Media may include paper, electronic, photographs, slides, audio and video. A Corporate Record is a non-clinical document which has been generated or received by the Trust and contains information that is **not** clinical care information.

Corporate Records relate to any records associated with Corporate business and should be retained as per the NHS Code of Practice for Records Management. They include:

- Business activity e.g. minutes, agenda's, correspondence, complaints, litigation, contracts, business continuity
- Supporting Judicial process e.g. Public Inquiries,
- Personnel e.g. personnel files, rostas, rota's registers
- Financial e.g. petty cash, budgets, accounts
- Estates e.g. leases, deeds, maintenance contracts

In some circumstances the Trust may be required to retain corporate and patient records for longer than the minimum record retention period, including temporary records, where they may have been due for destruction but are required to support litigation, public inquiries, on-going FOI requests or similar statutory reasons. In this event the Trust will agree local policy and procedure for the retention and management of the record/s and formally record such decision. The Trust will decide the retention period and establish a review of the timeframe for the retention to ensure that it is appropriate, compliant and meets statutory obligations.

There is a distinction between a record and a document. A document becomes a record when the document has been finalised. When it has been finalised it becomes part of the Corporate memory. A finalised and formal record makes information easier to manage in accordance with legislation and business need. Keeping an array of informal documents should be minimised as they are unlikely to meet any or all of the characteristics required for a corporate record and comply with legislation.

The Trust requires Corporate records for a number reasons and uses. These include:

- Support patient care and continuity of care
- Support improvements in clinical effectiveness through research
- Assist records audits
- Protect the interests of the Trust
- Protect the rights of patients and employees by providing evidence of patient care given

This Policy supported by a procedure will ensure the effective management of the lifecycle of Corporate information. It will ensure that information is saved and stored efficiently in a format and folder structure that allows easy retrieval and disclosure through to archival and destruction in line with NHS Records Retention schedule.

2. APPLICATION

This policy applies to all staff working within the Trust regardless of level or seniority including any individual directly employed or otherwise by the organisation for example, third party contracting staff, students, temporary staff, volunteers, locum or bank staff and any individual who has been given access to Trust network or systems.
.

Summary of role and responsibilities
N:B the following is a short summary of the role and responsibility. A full description of role and responsibilities can be found in the supporting procedure (SoP).

Chief Executive Officer (CEO)
The CEO has overall Trust accountability for this Policy and provides assurance to the Trust Board of statutory and regulatory compliance.

Senior Information Risk Owner (SIRO)
The SIRO is accountable for Information Risk Strategy and seeks assurance in respect of compliance with this Policy and procedure.

Caldicott Guardian (CG)
The CG is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The CG acts as the clinical conscience for the Trust.

Company Secretary
The Company Secretary will hold management accountability for Corporate Records and has a role to encourage services in the Trust to maintain high standards of corporate records management in accordance with the Policy and SoP.

Information Governance, Assurance and Compliance Lead
The IG Lead is responsible for ensuring that the organisation meets its statutory and corporate responsibilities and engenders public confidence in the handling of personal and corporate information.

Information Asset Owners (IAO) and Information Asset Administrators (IAA)

IAO and IAA's will also support the SIRO in the overall Information risk management function and ensure the use and protection of the Corporate asset. This will be achieved by maintaining an Information Asset register which is reviewed as a minimum annually.

The IAO and IAA roles will document, understand and monitor;

- What information assets are held and for what purpose
- How information is created, amended or added to overtime e.g. access to the correct version
- Who has access to the information and why
- Understand and address the risk to the asset, providing assurance to senior management

Managers
All managers within the Trust are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance.

Staff
All staff are required to familiarise themselves with the Policy and associated procedures and guidance and to comply with the expectations set out. Staff are expected to seek assistance from their line manager with any issues relating to compliance or understanding of the Policy or associated documents.

This policy applies to the governance of Corporate information, produced, stored, used, shared and transferred by the Trust including:

- Non Clinical patient information
- Human resources information
- Finance information
- Property Services and Facilities Management information
- Corporate Governance information
- Organisational administrative information

This Policy covers:

- All staff of the organisation, including temporary staff and contractors, sub-contractors;
- All Corporate information used by the organisation;
- All Corporate information systems managed by or used by the organisation;
- Any individual using Corporate information "owned" by the organisation;
- Any individual requiring access to Corporate information "owned" by the organisation.

3. IMPLEMENTATION

In order to comply with the Policy staff must ensure that they familiarise themselves with relevant policies and guidance and that they understand the responsibilities set out in them. If individuals are unsure about any aspect of a Policy or guidance they must seek clarification from their line manager, Corporate Governance and Compliance team or the Information Governance team. Staff must ensure that they are compliant with legislative and regulatory requirements on a day to day basis.

It is the role of the Chief Finance Officer / SIRO to ratify Trust Corporate policies in respect of IG Policies, taking into account legal and NHS requirements. The board is also responsible for ensuring that sufficient resources are provided to support requirements of this policy.

This Policy works in conjunction with other related Policies and Procedures e.g.

- Corporate Records Procedure
- Information Governance Policy and Procedure
- IM& Security Policy
- Freedom of Information Policy
- Business Continuity plans
- NHS Codes of Practice e.g. Records Management, Confidentiality

Policies can be found at
http://trustnet/docs/policies/DOCUMENTS%20POLICIES/Forms/corporate.aspx

All Managers are responsible for ensuring that the Policy and its supporting standards and guidance are built into local processes and that there is on-going compliance on a day to day basis. Any breaches or suspected breaches of confidentiality or information security including cyber security events must be referred for immediate investigation.

4. COMPLIANCE

The Information Governance Toolkit (IGT) includes three requirements related to Corporate Records Management specifically, Effective Corporate Records Management (601), Freedom of Information (603) and the Lifecycle of Corporate Records Management (604).

The IG team will work with managers and IAO's to establish an annual schedule of audits and to verify that the audits have been completed in order to satisfy compliance with IGT requirements. Managers and IAO's will be expected to identify any gap/s in practice and control and develop a remedial action plan to effect improvement.

Update reports will be provided to the Joint SIRO and CG Steering Group and as part of the Chairs report for the Corporate Governance and Compliance Sub Committee. Reports will also be used as evidence for the IGT.

Further scrutiny and monitoring of compliance with the requirement of the IGT and the overall Corporate Records management practices may also be applied by the rolling internal audit plan. This will be agreed with the Corporate Governance and Compliance team on an annual basis.

5. COMMUNICATION

The Policy and supporting documents will be circulated first by using the Trust Metacompliance software to ensure a majority communication. This method will provide a report of how many staff have received and agreed their understanding of it. The Policy will also be sent out using the Trust weekly news bulletin followed by the Policy and supporting documents being posted on the Trust intranet and Information Governance Sharepoint page.

It will be the responsibility of the IG Lead in conjunction with the Corporate Governance and Compliance team to ensure that the Policy and associated documents are kept up to date.

Training will be provided to staff for new Corporate Records Processes as required and where a need is identified.

A more detailed Communications Plan can be found in the supporting SoP.

6. MONITORING INTEGRITY OF THE SYSTEM

The Information Governance Lead (IG Lead) will ensure that any changes to Data Protection legislation or associated statutory, regulatory or NHS monitoring systems e.g. Information Governance Toolkit are advised and effected in this Policy. All changes will be reviewed and agreed by the SIRO or the Company Secretary prior to ratification.

The IGT includes two specific requirements that monitor compliance of Corporate Records management and the Freedom of Information Act. To ensure the achievement of a minimum level two attainment the IG team will collaborate with the Corporate Governance and Compliance Department, to oversee the completion of an annual Corporate Records Audit schedule. The initial findings will be shared with each Senior IAO for the Corporate service and the IAO's.

The results of the audit will be provided as evidence for the IGT annual submission and the audit report will be presented along with recommendations and an action plan if applicable to the Corporate Governance and Compliance Sub Committee as per the scheduled cycle of business.

In addition, the policy will be reviewed as part of a Corporate Policy risk assessment to ensure that the Policy remains fit for purpose and supports compliance with statutory legislation.