REF: PL012

Liverpool Women's NHS Foundation Trust

Management of Information Assets

Version	1.2
Designation of Policy Author(s)	Head of Information Governance and Records
Policy Development Contributor(s)	None
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date issued	01/04/2023
Review date	31/03/2024
Coverage	Trust Wide

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at www.nrls.npsa.nhs.uk/beingopen and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

CONTENTS Page

1 Executive Summary

1.1 Applicability and Scope

i. This policy covers all aspects of information within the organisation, including (but not limited to) patient/client/service user information, personnel information, organisational information

ii. This Policy covers all aspects of handing information within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information

iii. This Policy covers all Information systems purchased, developed and managed by/on behalf of, the organisation and any individual directly employed or any individual undertaking activity under the control or direction of the organisation

2 Introduction

i. The Trust regards all person identifiable information that it holds or processes as confidential and will implement and maintain policies to ensure compliance with all necessary mandatory obligations

ii. The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Effective information governance plays a key part in supporting clinical governance, service planning and performance management

iii. Effective Information Governance gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

iv. The Trust will ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management

3 Policy Objectives

i. To define the standards and Trust rules for all individuals for the management of Information Assets

4 Duties and Responsibilities

4.1 The Senior Information Risk Owner

- Is accountable for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control.
- Reviews and approve actions in respect of identified information risks
- Ensures that the organisation's approach to information risk is effective in terms of resource, commitment and execution
- Sets the overall objectives for Information Security for the Trust

4.2 Caldicott Guardian

- Is agreed as the 'conscience' of the organisation and to advise the Trust Board on matters relating to confidentiality.
- Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
- Approves the release of information where consent from the data subject is not considered necessary or appropriate

4.3 Chief Information Officer

- Has overall responsibility for Information Security for the Trust
- Ensures the overall approach taken to managing Information Security, Information Systems and Information technology is appropriate
- Supports the implementation of Information Security, Information Systems and Information technology overall objectives as directed by the Senior Information Risk Owner

4.4 Information Assets Owner

- Has responsibility for the safety and security of the Information Assets that they are responsible for
- Manages Information Governance and Information Security Risk associated with any Information Asset that they are responsible for
- Ensures that Information Governance and Information Security related incidents, that are attributable to the Information Asset that they are responsible for, are appropriately investigated

4.5 Head of Information Governance and Records

- Maintains and develops the Trust Information Governance and Information Security Policy and Framework.
- Manages Confidentiality and Data Protection across the Trust as the Subject Matter Expert
- Manages and Implements the Trust Information Asset Framework
- Implements the Information Governance related directives and objectives of the Senior Information Risk Owner

5 Main Provisions

5.1 General Provisions

i. The Trust will categorise its Information Assets according to the nature of the information asset and will align governance arrangements according to the nature of each of those Information Assets.

ii. Unless there are technical, or other significant reasons not to, all Information Assets shall be implemented in accordance with the Trust Data Manual

iii. Electronic Staff Record (ESR) shall be the reference system for data contained in all Information Assets, meaning that data in all Information Assets shall, where such data exists in ESR, use the same data structure, naming conventions and lookups.

iv. Unless there are technical, or other significant reasons not to, all Information Assets shall be implemented with Active Directory Login integration

5.2 Prioritisation of Information Assets

i. The Trust has categorised its Information assets as follows

Level	Definition
Level P1 (Critical Assets)	An Information Asset, without which: - There would be an immediate risk the health and wellbeing of patients, staff, visitors or any other service users, or - The Trust, or any department within it, would immediately be unable to carry out any of its statutory or other mandatory duties, or - The Trust, or any department within it would be immediately operationally halted
Level P2	An Information Asset, without which: - Operational activities are widely impacted upon but there is no immediate risk to the health and wellbeing of patients, staff, visitors or any other service users, or - The Trust, or any other department within it, would be widely operationally affected but would still be able to carry out its statutory or mandatory duties, or - The Trust, or any department within it, would be widely impacted upon but would remain operational.
Level P3	An Information Asset, without which: - Operational activities are not impacted upon, there is no risk to patients, staff, visitors or any other service users but the Trust, or any department within it, would be unable to function as it did before the Information asset became unavailable.
Level P4	All other Information Assets not categorised above

5.3 Requirements Associated with Information Assets

i. The following requirements shall be associated with each category of Information Asset

Level	Requirement
Level P1 (Critical Information Asset)	The Information Asset must have a System Level Security Policy that is approved by the Information Governance Committee every 3 years or when there is a significant change made to it Information Assets Owners and Administrators: - Will have completed supplementary Information Governance training, which will be kept is up to date
Level P2	The Information Asset must have a System Level Security Policy that is approved by the Information Governance Committee when it is introduced and

	when there is a significant change made to it Information Assets Owners and Administrators: - Will have completed supplementary Information Governance training, which will be kept up to date
Level P3	The Information Asset must have a System Level Security Policy that is approved by the Head of Information Governance or Information Assurance Manager when it is introduced and when there is a significant change made to it.
Level P4	The Information Asset Owner must have available, when requested, a summary of the information that would ordinarily be contained within System Level Security Policy, sufficient in detail to provide assurance to the SIRO that the asset in question is being effectively managed.

5.4 Allocation of Information Asset Owner

i. The Information Asset Owner for a Trust system shall be defined according to the following:

	System Description	Information Asset Owner	Information Asset Administrator (if relevant)
A	The system is used primarily within a single department, area or function for use primarily by that department, area or function	The most senior operational manager[1] of the department within which the system primarily operates	An individual named by the Information Asset Owner
B	The system is managed and controlled primarily by a single department, area or function and is used in more than one area of the Trust, or across the Trust	The most senior operational manager[1] of the department, area or function within which the Information Asset Administrator is employed	The individual within the department that provides day to day management of the system. E.g. Allocation of permissions, deactivation of users, modification to data
C	A system that is not managed or controlled primarily by a single department, function or area and is used in more than one area of the Trust, or across the Trust	In order of priority: 1) The person that signed the contract 2) The person that currently manages the contract 3) The person that signed or manages the Service Level Agreement 4) The person named within the Information Sharing Agreement for that Information Asset	An individual named by the Information Asset Owner
D	The system has been developed locally by an individual for use by	The person that developed the system	None

	themselves or by a limited number of individuals		

ii. Where any Information Asset is not covered by the above definitions then the relevant Information Asset Owner shall be assigned to an individual by the Senior Information Owner (SIRO)

iii. The Information Asset Owner may delegate responsibilities as Information Asset Owner so long as they:
- Accept that they are responsible for ensuring the individual to whom it is delegated is aware that it has been delegated
- Accept that they maintain accountability as Information Asset Owner and are responsible for ensuring the individual to whom it has been delegated undertakes what is required as (delegated) Information Asset Owner
- Ensure the Information Governance Department is aware when responsibilities have been delegated
- Accept that the individual to who a system is delegated must themselves be sufficiently senior to act as Delegated Information Asset Owner

iv. Where an Information Asset Owner has not delegated responsibility to a named individual, under the conditions specified above, the Information Asset Owner will retain responsibility for that Information Asset.

v. An Information Asset Owner to whom an Information Asset Owner has been delegated shall be known as a "Delegated Information Asset Owner" and will become the individual who will have day to day responsibility for that Information Asset Owner to the same extent as the Information Asset Owner themselves.

vi. The responsible person will remain as the Information Asset Owner, which is defined by the above and will not change.

5.5 Registration and Risk Assessment of Information Assets

i. All Information Asset Owners must ensure the Information Asset, which they are the owner of, is registered with the Information Governance Department.

5.6 Externally Hosted Systems and 3rd Party Suppliers

i. Information Assets Owners are responsible for ensuring that 3rd party hosted systems are equivalent in terms of safety, security and assurance, to the systems that are hosted directly by the Trust

5.7 Authority to Act

i. Approving Officers are, for the purposes of this Policy:
- Chief Information Officer
- Head of Information Governance and Records

ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer

iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest

iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Governance Committee at the first opportunity

5.7 Reporting

i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control

ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

6 Key References

i. The Data Protection Act 2018
ii. The General Data Protection Regulations
iii. The Information Security NHS Code of Practice
iv. The NHS Confidentiality Code of Practice
v. The Records Management NHS Code of Practice
vi. Freedom of Information Act 2000
vii. Data Security and Protection Toolkit
viii. The Computer Misuse Act

7 Associated Documents

None

8 Training

i. Training for implementation of this policy is contained within the Trust overall training program and is reference by the Information Governance and Information Security Policy and Framework

9 Policy Administration

9.1 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	17/11/2020	None

Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes	
External Stakeholders		
Trust Staff Consultation via Intranet	Start date: 17/11/2020	End Date: 17/12/2020

Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)	By Whom will this be Delivered?
The policy is existence already	

Version History

Date	Version	Author Name and Designation	Summary of Main Changes
17/11/2020	1.0	Russell Cowell, Head of Information Governance	New Policy
31/03/2022	1.1	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
31/03/2023	1.2	Russell Cowell, Head of Information Governance and Records	General wording review and re-approval by Information Governance Committee. Update to job title of Head of Information Governance to add "and Records" to title. Changes to the requirements associated with Information Assets (Paragraph 5.3)

10 Initial Equality Impact Assessment Screening Tool

Name of policy/ business or strategic plans/CIP programme: **Confidentiality Policy**	**Details of policy/service/business or strategic plan/CIP programme, etc:**	
Does the policy/service/CIP/strategic plan etc affect (please tick) **Both** X		
Does the proposal, service or document affect one group more or less favourable than another on the basis of:	**Yes/No**	**Justification/evidence and data source**
Age	No	All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity
Disability: including learning disability, physical, sensory or mental impairment.	No	
Gender reassignment	No	
Marriage or civil partnership	No	
Pregnancy or maternity	No	
Race	No	
Religion or belief	No	
Sex	No	
Sexual orientation	No	
Human Rights – are there any issues which might affect a person's human rights?		**Justification/evidence and data source**
Right to life	No	Obligations laid out within the policy are primarily defined by the Data Protection Act. All confidential information is treated equally and all monitoring systems are neutral in terms of their application against Equality and Diversity. There would be no impact on the Human Rights as the Policy is a direct reflection of legislation, which itself would have considered the impact on Human Rights
Right to freedom from degrading or humiliating treatment	No	
Right to privacy or family life	No	
Any other of the human rights?	No	
EIA carried out by: Quality assured by: PGP Meeting	01/04/2022	Russell Cowell, Head of Information Governance