Liverpool Women's
NHS Foundation Trust

Ref: PL004

Clear Desk Policy

Version	3.2
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 personal information within the organisation, including (but not limited to) patient/client/service user information, staff personnel information and 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 Trust and any individual directly employed or any individual undertaking activity under the control or direction of the Trust

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 personal information in the workplace

4 Duties and Responsibilities

4.1 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 Governance for the Trust

4.2 Caldicott Guardian

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

4.3 Chief Information Officer

- Has overall responsibility for the operation of Information Governance for the Trust
- Ensures the overall approach taken to managing Information Governance is appropriate
- Supports the implementation of Information Governance overall objectives as directed by the Senior Information Risk Owner

4.4 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.
- Is responsible for Subject Access and Freedom of Information requests.
- Implements the Information Governance related directives and objectives of the Senior Information Risk Owner

5 Main Provisions

5.1 General Provisions

i. All staff shall ensure that computer systems are locked for any period when those computers are left unattended. Portable devices that are the property of the Trust and are to remain on Trust premises overnight must be stored securely.

ii. All staff are required to secure all sensitive or confidential information in their workspace:
   a. at the end of each working day, or
   b. when they are expected to be away from their workspace for an extended period, or
   c. where leaving their workspace would leave sensitive or confidential information unattended

iii. All staff are responsible for ensuring that access to any area that contains confidential information is only granted to individuals who have an operational need to be there at that time and are authorised to enter that area

iv. All staff are responsible for ensuring that confidential information is not left unattended and unsecured, which applies to, but is not limited to, physical information, such as filing cabinets and electronic information such as information stored on computer systems

v. All Staff must ensure that no document containing confidential information is left anywhere where it can be viewed by anyone who does not have the authority or need to do so

vi. Staff are required to ensure that any printed materials are removed from printers or fax machines immediately after they have been printed and to ensure documents are managed electronically wherever possible.

vii. Staff are responsible for ensuring that items that are used to control access to confidential information, such as keys or physical access swipe cards, are not left unattended at any time

viii. The Trust will take appropriate action against any individual who has been found to have deliberately, or by deliberate omission of action, failed to maintain the minimum standards of conduct expected of them

ix. Unless specifically authorised to do so by an Approving Officer, no member of staff may hold any Trust related confidential information on a portable device, such as a mobile phone, portable hard drive, USB pen drive, tablet or laptop. Where authority has been given to hold Trust related confidential information on a portable device then the member of staff who has been authorised shall ensure that such devices are locked away when not in use.

5.2 Home and Remote Working

i. Any member of staff who is working from home or any other remote location shall comply fully with the provisions of the Confidentiality Policy

ii. Provisions regarding ensuring “clear desk” is maintained appllies equally at home (or any other remote working location) as they do within the premises of the Trust

5.3 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

5.4 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 UK General Data Protection Regulations
iii. The Information Security Management 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 1990

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	25/03/2020	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: March 2020		End Date: April 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?
Approval by Senior Information Risk Owner, uploaded to Intranet and Internet. Provisions to be assimilated into staff Information Governance Handbook	

Version History

Date	Version	Author Name and Designation	Summary of Main Changes
31/03/2020	1.0	Russell Cowell, Head of Information Governance	New Policy
31/03/2021	2.0	Russell Cowell, Head of Information Governance	General wording update to ensure that the policy is kept up to date with policy decisions taken and legislation. Section has been added relating to Home and Remote working. No other significant changes
31/03/2022	3.1	Russell Cowell, Head of Information Governance	Review only and re-approval. No changes
31/03/2023	3.2	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. Re-allocation of policy sponsorship to the Chief Information Officer

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** ☒		
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