NHS
Liverpool Women's
NHS Foundation Trust

Ref: PL010

Physical Server Protection and Physical Access Control

Version	3.2
Designation of Policy Author(s)	Head of Information Governance and Records
Policy Development Contributor(s)	Head of Technology
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.

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 involved in the physical protection of the Trust network infrastructure

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 and that this is communicated to all staff.
- 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

- Takes overall responsibility for IT Services for the Trust
- Ensures that the organisation complies with all mandatory requirements in respect of Information Technology, Information Security and Cyber Security
- 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 Head of Technology

- Is responsible for the management of Information Security across the Trust.
- Monitors local responses to Information Security incidents and provide support in developing proportionate and effective responses to manage risk.
- To be responsible, as operational Lead, for IT services and the associated security risks.
- Manages the Trust Information Technology infrastructure on a day to day basis as directed by the Chief Information Officer

5 Main Provisions

5.1 General Provisions

i. The Head of Technology will ensure the necessary physical safeguards are in place to protect the hardware of the Trust Network Infrastructure from compromise.

5.2 Access to Controlled Areas

i. Only individuals that have been approved by the Head of Technology may enter an area where the Trust network is housed or controlled

ii. The Head of Technology shall ensure an up to date list of named individuals who are authorised to access such areas is maintained. Where the individual is not an employee of the Trust, then a record of each instance where such an employee has accessed such areas, shall be maintained

iii. All individuals granted physical access to any area where the Trust network is controlled or housed are responsible for the protection of the network infrastructure for any period during which they are in the areas where the network is controlled or housed. Individuals who, by deliberate omission of action, fail to protect the Trust to its network infrastructure, may be subject to disciplinary action

iv. Staff may only enter an area where the Trust network is controlled or housed for activities relating to their role and for a specific purpose relating to that role

v. Where access to any area where the Trust network is controlled or housed is granted to an individual who is not employed by the Trust, the individual shall be accompanied at all times by an individual who are, themselves, authorised by the Head of Technology, to enter that area

vi. Suitably authorised individuals who are accompanying non-employees in an area where the Trust network is housed or controlled are personally responsible for the conduct of any individual who they are accompanying whilst they are in that controlled area

vii. Where access to any area, where the Trust network is controlled or housed, is granted to an individual who is not employed by the Trust, the individual shall be required to sign in when entering controlled areas

viii. Where access to any area, where the Trust network is controlled or housed, is granted to an individual who is not employed by the Trust, the individual shall, at all times, wear appropriate ID

5.3 Environmental and Physical Protections

i. All areas where the Trust network is controlled or housed shall be protected by appropriate physical access controls that will:
   - Ensure that protection is sufficiently robust so as to deter any unauthorised physical attempt to gain access
   - Ensure that protection is sufficient to allow only those authorised to enter the area to do so
   - Ensure sufficient monitoring systems are in place to confirm when the controlled area has been accessed
   - Ensure that, where a keycode is used to protect any controlled area, the keycode is changed on a regular basis

ii. Any area where the Trust network is controlled or housed shall be protected by Uninterruptable Power Supplies (UPS) that shall be suitable for the intended purpose and, in any case, will be suitable for a minimum of 10 minutes down-time

iii. Any area where the trust network is controlled or housed and requires temperature control shall be protected by temperature control systems that are appropriate for the intended purpose

iv. Any area where the trust network is controlled or housed shall be protected by fire control and protection systems that are appropriate for the intended purpose

v. Any area where the trust network is controlled or housed shall be suitable in physical design as to provide maximum protection against all reasonably considered eventualities

vi. All temperature control units have a pre-set temperature depending on the season. Changes to the ambient temperature may only be authorised by the Head of Technology

vii. The Head of Technology shall ensure effective monitoring systems are in place in areas where the Trust network infrastructure is controlled or housed in order to ensure optimal environmental conditions can be maintained and problems rectified as soon as possible

viii. Changes to the configuration of setting that is in relation to the physical control and protection of the Trust network infrastructure can only be made following authorisation by the Head of Technology

ix. Smoking, eating and drinking is not allowed in areas where the network infrastructure is controlled or housed

x. Access to the secondary data centre, on behalf of the Liverpool Women’s Hospital, must be approved by the Head of Technology

xi. Any member of staff entering any area where the Trust network infrastructure is controlled or housed is responsible for general housekeeping in that area. The Head of Technology will ensure each area is inspected and cleaned on a regular basis

5.4 Authority to Act

i. Approving Officers are, for the purposes of this Policy:
   - Chief Information Officer
   - Head of Technology
   - IT Operations Manager

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

5.5 Reporting and Monitoring

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 1988
ii. The UK 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	19/03/2018	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: January 2018		End Date: January 2018
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
21/08/2017	1.0	Russell Cowell, Head of Head of Information Governance	Policy has been completely reviewed and re-written. Policy version set to version 1.0 to reflect the substantial changes and the fact that it has been developed as an integrated policy set
03/09/2018	1.1	Russell Cowell, Head of Head of Information Governance	Periodic review. Minimal updates to wording and KPIs. Addition of IT Operations Manager as 'Approving Officer'

31/03/2020	2.0	Russell Cowell, Head of Head of Information Governance	General review and update to policy wording. Redefined categories in respect of legitimate activities when using Trust equipment, additional provisions for Bring Your own Device and staff response to suspicious Emails
31/03/2021	3.0	Russell Cowell, Head of Head of Information Governance	General wording update to ensure the policy is kept up to date with policy decisions taken and legislation. No 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