Liverpool Women's NHS Foundation Trust

Ref: PL006

# Access to and Monitoring of the Trust Network Infrastructure

| | |
|---|---|
| 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 | 31/03/2023 |
| 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 accessing the Trust network

# 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

- 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. Only individuals who have been provided with a username and password are authorised to access the Trust network.

ii. Individuals may only access the Trust network if they are sufficiently trained, are competent and can comply with all necessary obligations

iii. Access to the Trust network will be provided to individuals who have fully completed the necessary application forms. The IT Department is responsible for ensuring all necessary obligations have been complied with before granting access to the trust network

iv. No individual may have a user account for the Trust network if there is no formal contractual association between the individual and the Trust.

v. The Trust reserves the right to undertake any reasonable investigations to enforce the provisions of this policy

vi. The Trust reserves the right to suspend or terminate the access rights of any individual where there is reasonable belief that the user is not complying with any or all of the Trust policies or the user account has been compromised. Where such action is deemed to be necessary, it shall be approved by an Approving Officer

### 5.2 Conditions of Access

i. All individuals granted access to the Trust network have a personal responsibility to ensure that the login credentials are appropriately protected. Failure to apply appropriate protection for login credentials may be considered a disciplinary offence

ii. Staff may only access the Trust network for activities related to their role with the Trust and any other purpose that is explicitly required and approved by the Trust

iii. Staff are responsible for informing the Trust at the earliest opportunity where they have a reasonable belief that their access credentials have been compromised

iv. Staff must ensure that they access information systems only for purposes relating to their role and discharging their responsibilities in that role and are responsible for all activities undertaken on their accounts during times when their account was logged into the Trust network.

v. Members of staff who deliberately use another person's login credentials, or who share their login credentials, may be subject to disciplinary actions

vi. All members of staff in the Trust are responsible for contributing to the protection of the Trust network infrastructure that is commensurate with the responsibilities of their role and reasonable expectations of them as an employee.

vii. Employees must ensure they have logged off any machine when they leave their machine unattended and, in doing so, ensure that they render it not possible for another individual to access that computers system using their login.

viii. A member of staff who has logged into the Trust network will be responsible for all activities undertaken during that login session.

ix. All staff are responsible for ensuring that the IT Department is informed at the earliest opportunity where they have a reasonable belief that the Trust network infrastructure has been compromised.

x.

### 5.3 Ensuring Access is relevant and Up-To-Date

i. Where an individual's access requirements change, it is the responsibility of the individual user to inform IM&T of the change so that the user account may be updated accordingly

ii. Access rights to the Trust network will be allocated on the basis of the requirements of the individual and shall be proportionate to the individual's specific needs

### 5.4 Administrator or Super-User Accounts

i. Any individual who holds administration or super-user accounts shall have two accounts, one for non-administrator related activities and one for activities as an administrator. Individuals with such accounts shall be responsible for ensuring the correct account is used for the correct purpose

ii. Any individual who holds administrator privileges is required to change their password every 30 days and to ensure that their password:
    a. Has a minimum length of 12 characters.
    b. Is a mix of upper case, lower case, numbers and non-alphanumeric characters
    c. Does not contain all or part of the user name or job function

### 5.5 External Employees, Contractors and Other 3rd Party Suppliers

i. Access to the Trust network by individuals that are not directly employed by the Trust must be approved by an Approving Officer. Except as allowed under any other specific provisions elsewhere within this policy~~,~~ access for external employees, will only be provided for the period to undertake any necessary work

ii. An external employee may not be granted access to the Trust network unless and until the individual has completed the Trust Confidentiality Forms as specified in the Confidentiality Policy and the individual has been registered on the Leavers System. External employees must declare an expected end date for when access is expected to end. Where a date is not declared then, notwithstanding other information that would indicate that the individual had left before their scheduled end date, the individual's access will be deactivated automatically and without notice after 6 months. The necessary forms (FM001 and FM002) are available via Section 7.

iii. The Information Governance Department will maintain, through the Leavers System, a register of all users that are not directly employed by the trust and have been granted access to the Trust network.

iv. An application by an employee for access to the Trust network must be sponsored by an appropriate manager, who is an employee of the Liverpool Women's Hospital and is at Department Manager level or above. Access for external employees cannot be given for a continuous uninterrupted period exceeding 2 years. If the period of access reaches 2 years, then it is the individual's responsibility to re-apply for access. The Trust will accept no responsibility for users that have been deactivated as a result of a failure to submit a renewed application

v. External contractors and 3rd party suppliers, who are working for an organisation that supplies digital services to the Trust, must comply with all necessary obligations that will be specified at the time their services are needed or are contained within formal contractual documentation.

vi. Allocation of User Accounts

The following rules will apply to the creation of user accounts and Office 365 accounts

a. Where an individual is commissioned by the Liverpool Women's Hospital to provide a service then they shall be provided with the appropriate accounts, facilities and privileges that are needed for them to discharge their responsibilities that they have been commissioned to perform for the Trust

b. Where an individual, or the organisation they work for, has requested access to the Trust network then, if approved, they will be provided with a Trust Network Account only. Where they, or the organisation they work for, request supplementary facilities or privileges, the Trust reserve the right to pass on any cost to the Trust in providing those facilities or privileges

c. Requests for any Officer 365 services for students will be considered on a case by case basis, the granting of which will be at the sole discretion of the Trust.

### 5.6 Password Management

i. The Trust requires users to change their password every 42 days. Passwords must be 8 characters or more, be a mix of upper case, lower case, numbers and non-alphanumeric characters and not contain all or part of the user name or job function

ii. Sharing of usernames and passwords or otherwise allowing an individual uncontrolled access the Trust network is not allowed.

### 5.7 Intervention and Monitoring

i. The Trust may access any user account, or any software associated with that account, where this is considered operationally necessary or where there is a belief that a user account may be compromised. Where it is considered necessary to access a user account, due account will be taken of the privacy and human rights of the account holder. Where it is considered necessary to access an individual's ~~a~~ user account then the instance of access shall be approved by an Approving Officer

ii. The Trust will monitor network access as part of its normal activity to ensure users are acting in accordance with their obligations

### 5.8 Scheduled Termination or Suspension of Access

~~i.~~ The Information Governance Department shall be informed of the leaving date of all leavers or those users that are to have their accounts suspended which will be before the actual leaving date, and will provide the Information to IT Services. The user account will be deactivated or suspended on the first working day after the date the individual leaves.

### 5.9 Unscheduled Termination or Suspension of Access

i. Where the need arises to deactivate or suspend the user accounts of individuals who require immediate account deactivation or suspension, it is the responsibility of the relevant manager to inform the Information Governance Department as soon as the need to immediately deactivate or suspend the user is identified.

ii. It is the responsibility of the Information Governance Department to register the individual on the Leavers System and to inform system owners of the need to de-activate or suspend the user. Requests for immediate deactivation or suspension of user accounts shall be considered a priority and will be acted upon by system owners without undue delay and, in any case, within 30 minutes of being notified by the Information Governance Department.

### 5.10 Other Circumstances When Access is Terminated or Suspended

i. Where a user network account has not been logged into for 90 days then the account shall be reviewed and:
   a. Where it is considered necessary to maintain an active account then no action shall be taken
   b. Where it is considered not necessary to maintain an active account then the account shall be suspended

ii. Unless there are specific reasons not to, network accounts of users, having been reviewed as per Para 5.10.i (above), and where there has been no activity on that account for a further 185 days, shall be deactivated.

iii. The Head of Technology shall have discretion to suspend or deactivate user accounts:
   a. Where a user network account has been created and has never been logged into, or
   b. Where it a computer account is considered necessary to suspend or deactivate

### 5.11 Authority to Act

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

### 5.12 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

i. All associated documents are available via the Trust Intranet at:
http://imt012/Policies_Procedures_and_Guidelines/default.aspx

ii. Forms:
FM001 – General Confidentiality Form

## 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)<br>(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 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 Information Governance | Updated KPIs. Addition of IT Operations Manager as an Approving Officer |
| 31/03/2020 | 2.0 | Russell Cowell, Head of Information Governance | Major review and revision of wording considering lessons learned, introduction of new governance arrangements, insertion of GDPR related provisions and provisions following independent external review by Data Protection Officer |
| 04/12/2020 | 3.0 | Russell Cowell, Head of Information Governance | General review and minor update on policy wording to make provisions clearer based on experience. Enhancements to provisions on cyber security, re-organisation of paragraphs within policies (without word changing) so some text now moved into other policies and vice versa |
| 31/03/2022 | 3.1 | Russell Cowell, Head of Information Governance | Review only and re-approval. No changes |
| 31/03/2023 | 3.2 | 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:**<br><br>**Confidentiality Policy** | **Details of policy/service/business or strategic plan/CIP programme, etc:** | |
|---|---|---|
| **Does the policy/service/CIP/strategic plan etc affect (please tick)**<br><br>**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:<br><br>Quality assured by:<br>PGP Meeting | 01/04/2022 | Russell Cowell, Head of Information Governance |