

Cyber Security Policy

Version	3.3
Designation of Policy Author(s)	Head of Information Governance and Patient 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	01/04/2024
Review date	31/03/2025
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	3
	1.1 Applicability and Scope.....	3
2	Introduction	3
3	Policy Objectives	3
4	Duties and Responsibilities	3
5	Main Provisions	4
	5.1 General Provisions.....	4
	5.2 Reviewing Access Privileges	4
	5.3 Service Accounts	5
	5.4 Generic Accounts.....	5
	5.5 System Hardening, Patching and Security General Approach	5
	5.6 Externally Hosted Systems and Suppliers	7
	5.7 Servers and Server Software Maintenance and Repair	7
	5.8 External Network Connections.....	7
	5.9 Internet Monitoring and Filtering	7
	5.10 Monitoring Systems	7
	5.11 Virus and Malware Protection	7
	5.12 Redundant Equipment	8
	5.13 Authority to Act.....	8
	5.14 Reporting.....	8
6	Key References	9
7	Associated Documents	9
8	Training	9
9	Policy Administration	9
	9.1 Consultation, Communication and Implementation	9
10	Equality Impact Assessment	11

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 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 either directly or via a 3rd party through a formal contractual arrangement.
- iii. This Policy covers all Trust managed technologies including, but not limited to the Trust network, end user computing (EUC), devices (mobile phones, computer, tablets etc.), servers, backups, operating systems, and systems (application, software and databases)

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 safe and secure information, both in terms of the management of systems and the efficient management of services and resources. Effective information security plays a key part in supporting clinical governance, service planning and performance management
- iii. Effective Information security 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 security

3 Policy Objectives

- i. To define the standards and Trust rules for all individuals in respect of Cyber Security

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

4.3 Chief Information Officer

- Takes overall responsibility for IT Services for the Trust
- 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

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

- The Trust will deploy all reasonable and necessary safeguards to protect the Trust from compromise by Virus, Malware or any other cyber security threat to ensure maximum protection for the Trust network infrastructure.
- The Trust will ensure all necessary backups of the Trust network infrastructure are carried out to ensure maximum protection for the Trust network infrastructure. Backup processes and schedules will be implemented in accordance with the Trust backup policy.
- The Trust will ensure that the Trust virus protection and Firewalls are configured, maintained, and are kept sufficiently updated to ensure maximum protection for the Trust network infrastructure.
- The Trust will ensure that all information technology related maintenance contracts, which protect the Trust network infrastructure, are valid, current, relevant, appropriate, and sufficient to ensure maximum protection for the Trust network infrastructure.
- The Trust will ensure that, where standards are to be implemented, that there shall be no differential made between those that are directly employed by the Trust and those that are not, regardless of who they are employed by or the nature of their work
- Unless there are specific reasons not to, the Trust will adopt two-factor authentication on all systems and in all circumstances. Where this is not possible then the Trust will implement supplemental technical controls in order to optimise information security.

5.2 Reviewing Access Privileges

- i. The Head of Technology will ensure that the access rights that individuals have been granted is reviewed on a periodic basis to ensure the rights granted are up to date according to the role they are in.
- ii. The Head of Technology will ensure that administrator and super-user accounts are reviewed on a regular basis to ensure that all individuals that have such accounts should have those accounts. The review will, as a minimum, be conducted quarterly.
- iii. The Head of Technology will ensure that Service accounts are reviewed on a regular basis to ensure that they are still active accounts, are still required and are not dormant. The review will, as a minimum, be conducted quarterly.
- iv. The Head of Technology will ensure that generic accounts are reviewed on a regular basis to ensure that they are still active accounts and have not, by their nature, created any additional information security risks since they were last reviewed. The review will, as a minimum, be conducted quarterly.

5.3 Service Accounts

- i. A service account, which is a user account created explicitly to provide a security context for services running on operating systems. The security context determines the service's ability to access local and network resources.
- ii. Service accounts, which are user accounts created explicitly to provide security context for services running on operating systems, can only be given by an Approving Officer.

5.4 Generic Accounts

- i. Generic accounts, which are user accounts created explicitly to provide access to a device or system, will, themselves, have their own independent non-generic authentication.
- ii. Approval for the creation of generic accounts can only be given by an Approving Officer

5.5 System Hardening, Patching and Security General Approach

- i. Access Controls
 - a. The Trust will ensure that it complies with established best practice guidelines in respect of the management of passwords and lockout times.
 - b. Guest accounts shall be either disabled or renamed and default passwords shall be changed regularly and frequently
- ii. Security Patching (Update Installation)
 - a. The Trust will deploy patching onto all servers, end user devices, mobile devices, medical devices, and the network infrastructure. Patching shall be carried out on demand, as required, or as scheduled in order to ensure optimal system security.
 - b. Issues that may require escalation shall be escalated as considered necessary by Digital Services Management

iii. Network Configuration and Protection

- a. The Trust will ensure that devices and systems are protected by Firewalls. Key devices (i.e., server, firewalls, and printers) will, where necessary, have a static Internet Protocol (IP) address so that clients can reliably find them.
- b. Unnecessary IP ports will be disabled and firewalls rules will be regularly reviewed and documented.

iv. Encryption

- a. Encryption will be implemented to protect data in transit and at rest and will be regularly reviewed.

v. Remote Administration and Access

- a. Only approved administrators will be allowed access to configure or control Trust devices and systems. 3rd party administrators will use an appropriate and Trust approved tool when accessing Trust devices for administrative purposes. Access will be restricted to key directories on servers and computers

vi. Software and Programmes

- a. Where appropriate and necessary, anti-virus software will be installed, and unnecessary programmes will be removed. Unsupported software shall be updated to a supported version, or the software will be removed unless there are over-riding operational reasons not to.
- b. The Senior Information Risk Owner shall approve the continued use of unsupported software. Where there is more than one version of the same application then they can continue to be used so long as they continue to be supported or have been given approval to continue to be used by the Senior Information Risk Owner

vii. Services

- a. Unnecessary services will be disabled

viii. Databases

- a. For SQL Server databases, the System Administrator (SA) account shall not be used and will, where identified, be renamed and disabled. Native Windows Authentication will be enabled where possible and Mixed Mode Authentication will be disabled where Native Windows Authentication is enabled.
- b. Internal SQL accounts shall, for the purposes of password standards, be considered privileged accounts. Internal SQL logging shall be configured to alert on excessive failed logons.
- c. Guest accounts shall be removed or disabled having taken due account of any migrations where there is a risk that settings are inadvertently replicated. Legacy account will be removed when no longer needed. ODBC access will be constrained to specific IP ranges

ix. System Auditing and Monitoring

- a. Unless there are legitimate operational needs to do so and there is evidence of appropriate authorisation, changes shall only proceed where approval has been granted by the Change Advisory Board (CAB). Appropriate logging and monitoring shall be enabled to support the investigation, remediation, and rectification of identified issues.

- x. Device and System Backup
 - a. Devices and systems that require backup will be backed up

5.6 Externally Hosted Systems and Suppliers

- i. In terms of the implementation of Information Governance and Information Security standards, the Trust will make no differentiation between internally hosted systems and externally hosted system.
- ii. Information Asset Owners, who are responsible for the managing risk and assurance of externally hosted systems are responsible for ensuring that such equivalence is implemented via the management of Information Assets

5.7 Servers and Server Software Maintenance and Repair

- i. Only individuals who are authorised to have access to, or carry out any work on, any aspect of control of the network infrastructure may interact with any aspect of control of the network infrastructure.
- ii. The Head of Technology will ensure that adequate logs are maintained of who has authority to make changes to any aspect of the Trust network.

5.8 External Network Connections

- i The Head of Technology will ensure that all necessary technical security measures are in place on the Trust systems to ensure that external connections are secure-

5.9 Internet Monitoring and Filtering

- i. The Head of Technology will ensure that effective Internet monitoring and filtering systems are in place and will ensure such systems are kept up to date

5.10 Monitoring Systems

- i. The Head of Technology will ensure that the trust has sufficient monitoring systems in place to identify potential security threats
- ii. The Head of Technology will implement sufficient network monitoring tools to provide assurance to the Trust that it is able to detect, eliminate and minimise the effect of potential threats as quickly as possible

5.11 Virus and Malware Protection

- i. The Trust will:
 - a. Deploy anti-virus / anti-malware software across the whole of the Trust network infrastructure. The Head of Technology is responsible for the integrity and adequacy of the anti-virus / anti-malware software
 - b. Ensure that, where a device is reconnected to the network after a period of disconnected working, then it will be updated with the latest anti-virus and anti-malware definitions.

- c. Remove any device that is found to not have adequate protection until such a time as adequate protection has been applied
 - d. In the event of a virus outbreak or malware incident, remove equipment, disable user accounts or disable parts of the network as IM&T Management consider necessary.
 - e. Ensure that scanning is conducted in real time (on demand or on execution) and undertakes a full scan on a weekly basis
 - f. That, where virus / malware definitions are updated, then they are pulled from a secure and trusted source
 - g. The anti-virus / anti-malware software shall be configured to:
 - i. alert the IM&T team as soon as a virus or malware has been discovered
 - ii. quarantine or delete the virus or malware automatically
 - iii. exclude specific files or folders where scanning would potentially impact of the overall system performance
 - iv. Maintain logs for a sufficient period of time to allow for investigations into any incident that may have occurred
- ii. "CareCert" alerts produced by NHS Digital shall be acted upon in accordance with the requirements of any supervisory authority such as NHS Digital.

5.12 Redundant Equipment

- i. The Head of Technology will ensure that procedures are in place to ensure the safe and secure disposal of redundant equipment, including any information contained on it, to ensure the Trust is not placed at risk from a breach from an inappropriate or ineffective disposal of redundant equipment.

5.13 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

5.14 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	14/02/2023	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: February 2023		End Date: February 2023
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 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	Periodic review with minimal wording update and KPI review. Addition of IT Operations Manager as '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 definitions 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	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
31/03/2024	3.3	Russell Cowell, Head of Information Governance and Patient Records	General wording review and re-approval by Information Governance Committee. Minimal changes.

10 Equality Impact Assessment

Does The Policy Affect:	Staff		Patients		Both	X
--------------------------------	--------------	--	-----------------	--	-------------	----------

Equality Group	Impact (Positive/Negative/Neutral)
Race (All Ethnic Group)	Neutral
Disability (Inc Physical, long term health conditions & Mental Impairments)	Neutral
Sex	Neutral
Gender Re-Assignment	Neutral
Religion Or Belief	Neutral
Sexual Orientation	Neutral
Age	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Other e.g., caring responsibilities, human rights etc.	Neutral

For each protected characteristic, consider whether the impact is positive. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)

Not Applicable

For each protected characteristic, consider whether the impact is negative. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)

Not Applicable

If your assessment has identified any negative impacts, please detail any actions that have been put in place to mitigate these (upon approval of EIA these actions will be shared with the Equality, Diversity and Inclusion Committee):

Outcome	Actions Required	Time Scale	Responsible Officer

Is there evidence that the s. 149 Public Sector Equality Duties (PSEDs) will be met? Consider whether the proposed policy will...

- Eliminate discrimination, victimisation, harassment, and any unlawful conduct that is prohibited under this act
- Advance Equality of opportunity
- Remove or minimise disadvantages suffered by people who share a relevant protected characteristic that are connected to that characteristic
- Take steps to meet the needs of people who share a relevant protected characteristic that are different from the needs of people who do not share it
- Encourage people who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such people is disproportionately low.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. (Consider whether this is engaged. If engaged, consider how the project tackles prejudice and promotes understanding - between the protected characteristics)

Explain your answers below.

The policy is an administrative policy, which implements established legal obligations neutrally.

Does the EIA have regard to the need to reduce inequalities for patients with access to health services and the outcomes achieved? (this section is a requirement for any services outlined within the NHS England and Improvement [Core 20 Plus 5](#) approach to health inequalities) Explain.

The policy is an administrative policy, which implements established legal obligations neutrally.

Section 2:

To be completed by the EDI Manager authorising the EIA

Anything for noting or any recommendations for consideration by the Board

Guidance Note: Will PSEDs be met? Are Core 20 Plus 5 services considering patient health inequalities?

Review Date:

Additional Supporting Evidence and Comments: