Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Policy Title: Joint Information & Cyber Security Policy

Reference	POL/IG/008
Version	1.0
Date Ratified	31/10/2018
Next Review Date	31/10/2021
Accountable Director	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)
Policy Author	Derrick Bates

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

This document defines the overarching Joint Information & Cyber Security Policy of the Cumbria Partnership NHS Foundation Trust and of North Cumbria University Hospitals NHS Trust. It provides the foundation for thematic and supportive Information & Cyber Security Policies covering different aspects of information & cyber security – such as Acceptable Use, Forensic Readiness and Management of Information Risk.

Users must always comply with the rules laid down in this Policy when using Trust information processing facilities. Users must also remember that, it is not just in electronic processing, but in verbal and written communication that risk is involved and breaches may occur.

TARGET AUDIENCE:

- All Trusts' employees, consultants, third parties, contractors and temporary workers using Trusts' systems
- All Partner Organisations delivering services on behalf of the Trusts and using Trusts' systems and others who have been given access to internal Trusts' systems in support of service delivery.

TRAINING:

- Employee Induction
- Mandatory Data Security Awareness training using the Trust TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1

KEY REQUIREMENTS

1. Users must always comply with the rules laid down in this Policy when using Trust information processing facilities.

2. Users must also remember that, it is not just in electronic processing, but in verbal and written communication that risk is involved and breaches may occur.

3. Managers must ensure all staff members are aware of and in compliance with this Policy. This includes Cyber Awareness training.

4. Managers must also ensure that any potential disciplinary action with regard to the use or misuse of information processing facilities is investigated with this Policy in mind.

Contents

1. INTRODUCTION

Information held in electronic and manual information systems within the Trusts represents one of the Trusts' most valuable assets. It is, therefore, essential that all computers, networks and information contained within them are protected against the many threats which may compromise the data, patient or staff privacy.

Demands on services vary but the scope of providing services that meet each organisation's requirement for information system security remains the same. Each organisation (i.e. The Trusts and any contractors) must recognise and accept their responsibilities for the security of their assets.

This Information & Cyber Security Policy is the overarching document within the scope of the Information Security Management System (ISMS) and covers the information, information systems, networks, physical environment and relevant people who support the Trusts' business functions.

This document:

- Sets out the organisations' policy for the protection of the confidentiality, integrity and availability of their assets, including hardware, software and information handled by information systems, networks, applications and staff members
- Establishes the security responsibilities for information & cyber security
- Provides reference to additional relevant documentation

It is therefore supported by other policies and procedures dealing with specific functional areas and requirements such as Acceptable Use, Forensic Readiness and the Management of Information Risk.

2. PURPOSE

The purpose of this Policy is to ensure the security of the information assets of the Cumbria Partnership NHS Foundation Trust and of North Cumbria University Hospitals NHS Trust by implementing a suitable set of controls, including but not limited to policies, standards, practices, procedures, organisational structures and software functions, which reflect and meet the business need, and which will achieve an assessable standard of compliance with the relevant regulation and legislation.

Information & Cyber Security is characterised here as the preservation of:

- Confidentiality – ensuring that information is accessible only to those authorised to have access
- Integrity – safeguarding the accuracy and completeness of information and processing methods
- Availability – ensuring that authorised users have access to information and associated assets when required

3. POLICY DETAILS

Both Trusts will carry out security risk assessments in relation to all the business processes covered by this policy which will cover all information systems, applications and networks that are used to support those business processes.

It is mandatory under the General Data Protection Regulation (GDPR) for a Data Protection Impact Assessment (DPIA) to be undertaken when new technologies are introduced and on all changes in process or new processes that are required in order to ensure Confidentiality, Integrity and Availability of information and ensure rights and freedom of individuals. It is also mandatory for all departments to conduct a record of processing activities in order to meet accountability principles.

The principle objectives of the Policy are shown below:

- To preserve the confidentiality, integrity and availability of information within the Trusts
- To provide management direction and support for information & cyber security
- To ensure all information is adequately protected against loss, unauthorised access, disclosure or inaccuracy to allow the continuation of day to day core operations without loss or reduction to the quality of service
- To identify the threats to information assets, including vulnerabilities and their impact
- To ensure cyber security is an integral part of working with information.
- To ensure there is compliance with relevant legislation relating to the collection, maintenance and protection of information
- Access to information (whether manual or electronic) is to be made available only to those who require it in order to carry out their role
- To ensure all information security breaches, actual or suspected, are reported and investigated by the Information Security Managers
- To ensure networks are appropriately managed maintained and controlled in order that information that resides or flows within the supporting infrastructure is protected from vulnerabilities and threats
- To ensure that the both Trusts maintain the security of their systems and applications and any information in transit to external agencies

Further security objectives concerning matters such as Acceptable Use of Information Systems, Networks, Email, Mobile Devices, Information Risk and Social Networking are covered by thematic Policies in support of this overall Information & Cyber Security Policy.

Breaches of Information & Cyber Security are to be recorded on both Trusts' Ulysses Incident Systems. Any doubt as to what may constitute an incident should be referred to the relevant Trust's Incident Management Policy.

4. TRAINING AND SUPPORT

In order to ensure the correct implementation of this policy all managers are required to ensure that all their staff members are aware and have understood its content as part of approval of registration applications.

Information Asset Owners and Administrators should undertake regular information risk management training to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the organisation.

The following training requirements are specific to this policy:

- Employee Induction
- Mandatory Data Security Awareness training using the Trust TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1

5. PROCESS FOR MONITORING COMPLIANCE

The table below outlines the Trusts' monitoring arrangements for this policy/document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
On-going review of Information Security Elements – concerns and issues highlighted to the Board.	Cumbria Cyber Security Group and Joint IG Board reviews	Head of IG	Joint IG Board	Quarterly
Information Security Incidents	Ulysses Reports SIRI Reports	Head of IG	Joint IG Board	Quarterly
Spot checks on Policy compliance and knowledge on a % sample of employees	Monthly spot checks – results to be presented to the IG Board	Head of IG	Joint IG Board	Quarterly

<u>Wherever the above monitoring has identified deficiencies, the following must be in place:</u>

- Action plan
- Progress of action plan monitored by the Joint Information Governance Board minutes

- Risks will be considered for inclusion in the appropriate risk registers

7. REFERENCES:

Information Security Management NHS Code of Practice
https://digital.nhs.uk/article/1201/Information-security-management-NHS-code-of-practice

Codes of practice for handling information in health & care
https://digital.nhs.uk/codes-of-practice-handling-information

NHS Digital
https://digital.nhs.uk/

National Cyber Security Centre
https://www.ncsc.gov.uk/

8. ASSOCIATED DOCUMENTATION:

Information on the topics listed below can be found on individual Trust Intranet pages. Direct hyperlinks have been removed due to accessibility issues during the integration. If in doubt please contact the relevant IT Service Desk or IG Officers.

CPFT Intranet: http://cptportal.cumbria.nhs.uk/Pages/Home.aspx
NCUHT Intranet: http://nww.staffweb.cumbria.nhs.uk/index.aspx

- Information and Cyber Security Guidance
- Information and Cyber Security Policy
- Information Security Acceptable Use Policy
- Information Risk Policy
- Disciplinary Procedure
- Policy for the Use of Social Networking Sites.

9. DUTIES (ROLES & RESPONSIBILITIES):

9.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trusts, including ensuring that Trusts' policies comply with all legal, statutory and good practice requirements.

9.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates) & Senior Information Risk Owner (SIRO) Responsibilities:

All policies have a designated Executive Director and it is their responsibility to be involved in the development and sign off of the policies, this should ensure that Trust policies meet statutory legislation and guidance where appropriate. They must ensure the policies are kept up to date by the relevant author and approved at the appropriate committee.

The SIRO has responsibility for ensuring that an Information Risk Policy and Strategy is in place, and for assuring the Joint Trust Board of compliance with

relevant legislative and mandated requirements. The SIRO has overall responsibility to ensure an Information & Cyber Security Policy is in place, including processes to monitor such use, thereby providing assurance that management of threats to security is in place, and that all employees are aware of their responsibilities

9.3 Associate Medical Director/Caldicott Guardian Responsibilities:

The Caldicott Guardian is appointed by the Trust Board and registered with NHS Digital. He ensures that the Trust achieves the highest standards for handling patient information. He represents and champions patient confidentiality issues within the Trust's overall Information Governance Framework

9.4 Business Managers' Responsibilities:

Business Managers must ensure that they have agreed and implemented the departmental arrangements for ensuring compliance with this policy and all policies that are related.

Managers are responsible also for ensuring adequate dissemination and implementation of Policies relevant to the staff in their areas. If applicable, managers must ensure staff can access the hard copy policy summary file on their ward / department and ensure staff members understand how to access policies on the Intranet.

9.5 Joint Information Governance Board Responsibilities:

The Joint Information Governance Board (JIGB) is responsible for reviewing this Policy, ensuring it is fit for purpose and that it is ratified and passed for publication. The Chair of the JIGB will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

The Head of Information Governance reviews Information Governance incidents reported through the Trusts' Risk Management systems with this Policy in mind. The Head of Information Governance reports Serious IG Incidents to the JIGB. To further support the tenets of this Policy the Head of Information Governance reviews the Trusts' Information Flow Mapping on an annual basis, and reports any 'high risk' flows to the JIGB.

9.6 Trust Information Security Managers' Responsibilities

The Trust Information & Cyber Security Managers are responsible for:

- Acting as a central point of contact on information & cyber security within the organisations, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- The formulation, provision and maintenance of Information & Cyber Security Policies.

- Advising on the content and implementation of the Information & Cyber Security Programme.
- Producing organisational standards, procedures and guidance on Information & Cyber Security matters for review by the Caldicott Guardians and other senior staff represented on the JIGB, and other Governance Committees, on behalf of the Joint Trust Board,.
- Co-ordinating information & cyber security activities particularly those related to shared information systems or IT infrastructures.
- Liaising with external organisations on information & cyber security matters, including representing the organisations in cross-community issues.
- Ensuring that contingency plans and disaster recovery plans are reviewed and tested on a regular basis.
- Representing the organisations on internal and external bodies that relate to security.
- Ensuring the system, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally.
- Approving System Level Security Policies (SLSP) for the infrastructure and common services.
- Providing an incident and alert reporting system.
- Maintain contact with special Interest Groups in order to:

    - Keep abreast of “best practice”.
    - Maintain current knowledge of security-related matters.
    - Receive early warnings, alerts, advisories, etc. pertaining to developing threats[1].
    - Gain access to specialist advice.
    - Share and exchange information about new technologies, new threats, products, vulnerabilities, etc.

- Providing advice and guidance to Information Governance and users where applicable on:

    - Policy Compliance
    - Incident Investigation
    - Security Awareness
    - Security Training
    - Systems Accreditation
    - Security of External Service Provision

9.7 Information Asset Owners/Administrators

Systems and procedures must be put in place for each asset for which they are responsible thus enabling all employees to co-operate in the achievement of these objectives, including business contingency plans in the event of system unavailability.

[1] Such as the NHS Digital CareCERT Information sharing Portal

Information Asset Owners are responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Knowing what information comprises or is associated with the asset, and understanding the nature and justification of information flows to and from the asset
- Knowing who has access to the asset and why, whether it be system or information to ensure access is monitored and compliant with policy;
- Understanding and addressing risks to the asset, and providing assurance to the Senior Information Risk Owner.

9.8 Staff Responsibilities:

All staff members are responsible for reading and co-operating with the contents of this Policy as part of their normal duties and responsibilities. They are responsible for ensuring that they maintain up to date awareness of Information & Cyber Security practices with regard to their own and their staff roles and responsibilities. This includes the responsibility to report information security incidents as soon as they occur.

10. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
IAA	Information Asset Administrator
IAO	Information Asset Owner
IG	Information Governance
JIGB	Joint Information Governance Board
SIRO	Senior Information Risk Owner
SLSP	A documentation set created for each information asset and managed by the system IAO and IAA.

TERM USED	DEFINITION
CareCERT	An arm within NHS Digital that provides advice, alerts and weekly bulletins. It is also the main upward reporting point in the event of a serious cyber incident occurring
Information Asset	A system of data capture/maintenance that has value to the organisation, its business operations and its continuity (includes paper record systems/electronic systems/equipment etc.)
Staff	Full or part time employees, contractors, volunteers or third parties that work on behalf of the Trust.

11. DOCUMENT CONTROL

Equality Impact Assessment Date	N/A
Sub-Committee & Approval Date	Joint Information Governance Board – 21/09/2018

History of previous published versions of this document:

Trust	Version	Ratified Date	Review Date	Date Published	Disposal Date
NCUH - Information and Cyber Security Policy IG 20	v5	Dec 2016	Dec 2019	Dec 2016	-
CPFT Information Security Policy 002/077	vFeb16	Feb 2016	Mar 2019	Feb 2016	-

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1 Draft	09/02/2018	• Both Trust Information Security policies combined into new joint template • This Policy will replace both when published
0.2 Draft	21/02/2018	• Policy text moved into next new joint template.
0.3 Draft	20/07/2018	• Amended Accountable Director to reflect post rather than incumbent • Added minor amendments from CPFT Security Team. • Added amendments to Section 3 from Head of IG for GDPR inclusion.
0.3 Draft	11/10/2018	• Policy checklist completed

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Michael Smillie	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)/Senior Information Risk Owner	17/08/2018
Robin Andrews	Interim Executive Director of Finance	17/08/2018
Andrew Brittlebank	Medical Director	17/08/2018
Graham Putnam	Associate Medical Director/Chief Clinical Information Officer	17/08/2018
Dave Dagnan	Consultant Clinical Psychologist	17/08/2018

Name	Job Title	Date
Farouq Din	Associate Director of Digital Health	17/08/2018
Daniel Scheffer	Associate Director for Corporate Governance/Company Secretary	17/08/2018
Lesley Paterson	Associate Director of Quality & Nursing (Specialist Services)	17/08/2018
Lyn Moore	Associate Director of Operations	17/08/2018
Mandy Annis	Employment Services Bureau Manager	17/08/2018
Julie Thompson	Head of Workforce Services	17/08/2018
Elizabeth Klein	Head of Nursing - Clinical Standards	17/08/2018
Jacky Stockdale	Joint Business Manager - Corporate Services	17/08/2018
Paula McBride	Deputy Business Manager	17/08/2018
Kirsty Jay	Deputy Business Manager	17/08/2018
Laura Parkinson	Head of PMO	17/08/2018
Yvonne Salkeld	Head of IG	17/08/2018
Steve Johnstone	Joint Interim Head of IT	17/08/2018
Alan Lillie	CoIN Strategic Lead	17/08/2018
Lorraine Gray	Head of Information	17/08/2018
Natalie Karam	Head of Performance	17/08/2018
David Franklin	Financial Systems Manager	17/08/2018
Kath Watts	Network Manager - First Step	17/08/2018
Katherine McGleenan	Clinical Quality Manager	17/08/2018
Anne Gadsden	Information Governance Officer	17/08/2018
Paul Corrie	Information Governance Compliance Manager	17/08/2018
All NCUH Business Managers		17/08/2018