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

Policy Title: Joint Information & Cyber Security Acceptable Use Policy

Reference	POL/IG/007
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 policy has been developed to assist users in understanding what constitutes prohibited behaviour when using Trust information processing facilities to ensure that the same standard is used throughout the Trusts.

This policy includes a table to be used as a guide for managers in determining what inappropriate behaviour may need to be investigated. It is not exhaustive so advice may be sought from the Information & Cyber Security Managers

TARGET AUDIENCE:

- All Trust employees, consultants, third parties, contractors and temporary workers using Trust systems
- All partner organisations delivering services on behalf of the Trust and using Trust systems and others who have been given access to internal Trust 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 breaches may occur.

3. Managers must ensure all staff are aware of and are in compliance with this Policy.

4. Managers must ensure that staff members complete and acknowledge this Policy on the Electronic User Details form displayed at the beginning of each month on Trust PC's.

5. 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

This document defines the Trust's policy for the acceptable use of its Information Systems facilities. It relates to the use and monitoring of all of the Trust's Information Communication Technologies (I.C.T.), data communications and non-data communications systems.

It includes, but is not limited to, telephones, mobile telephones, smartphones, facsimile machines, computers (including laptops, tablets, smart devices, Internet of Things, wearables and personal organisers), portable data storage devices, Email, the Internet, Intranet, Extranet and any information resources processed thereon.

Effective security is a team effort involving the participation and support of every Joint Trust employee and any non-employee who deals with information and/or information systems on behalf of the Trusts. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. PURPOSE

This document defines the Trusts' policy on acceptable behaviour whilst using Trust information systems and is intended as a guide for users and managers.

The Trusts recognise that computer based information systems and services have the potential for enormous benefit to employees. The facilities give tremendous support to the management and delivery of Trust services and for communicating with partner organisations and stakeholders. However, the Trusts also recognise that misuse of ICT Systems and services is a risk that must be addressed by ensuring this Acceptable Use Policy (AUP) is embedded and complied with throughout the Trust.

3. POLICY DETAILS

3.1 Acceptable Use:

Acceptable use of the Trust's Information Systems is defined as its use in support of the Trust's clinical, statutory, business and service delivery activities, and those that do not come under the category of prohibited.

Users must always maintain a robust password for access to network systems using current Trust guidelines.

Users are permitted to use the Trust's Internet access for personal browsing with the following caveats:

- Explicit permission for personal browsing must be obtained from the user's Line Manager prior to use
- Personal browsing must not occur during the user's core working hours
- The prohibitions in Appendix 1 fully apply to personal browsing

The table showing all categories of prohibited use can be found in Appendix 1. It should be noted that some web sites that are not business related are routinely blocked. Request to unblock websites will only be considered where there is a business need.

3.2 Protocol on Other Uses:

Where Information Systems are to be used for purposes other than Acceptable Use as defined by this Policy, that use must be authorised in advance by the user's Line Manager with advice from the Information Security Manager. The Information Security Manager must also ensure that other appropriate permissions are also granted or denied as required. This includes, but is not limited to, the Caldicott Guardian and Data Protection Officer.

3.3 Applicable Regulatory Framework:

Users are bound by the Law of England and Wales when using the Trusts' Information Systems. In addition, when accessing computers abroad, the laws of that country apply. It is the user's responsibility to ensure his or her activities comply with these laws. The Trust can assist in the provision of guidance to relevant domestic legislation.

Users are also bound by the provisions of the General Data Protection Regulation (GDPR) This is to ensure the Confidentiality, Integrity and Availability of the Trusts' processes and to ensure the rights and freedoms of individuals.

Users must adhere to the applicable Codes of Conduct of any professional body to which they belong.

The use of the Trust's Information Systems is subject to all relevant Trust policies and regulations.

3.4 Prevention of Misuse:

The Trust retains a right of access to all information held on its Information Systems for the purposes of the protection of patients and staff and of investigating misuse. This may include, where criminal activity is suspected information held in folders that individuals have marked 'personal' or 'private'.

Monitoring may take place periodically within the guidelines set down by the Regulation of Investigatory Powers Act 2000 ('RIPA'), the Human Rights Act 1998 and the Data Protection Act 2018. The Trust retains the right supported by the ICO's Employment Practices Code to access all business related information held on its Information Systems to monitor system logs, web pages, e-mail messages, network accounts or any other data on any computer system owned or operated by the Trust. This is for the purpose of:

- Protecting patients and staff
- Ensuring personal information is being respected and protected

- Preventing, detecting or investigating crime or misuse
- Ascertaining compliance with regulatory standards and Trust Policies
- Ensuring effective system operation.

The privacy of all users must be respected at all times.

In order to guard against abuse of the Information Systems facilities Internet use is constantly monitored, email is scanned for profanity and other inappropriate content and the use of corporate telephony may be subject to investigation at any time, particularly when there is reason to believe that misuse is occurring. The Trust's policy on the prevention of misuse is to:

- make all employees, consultants, temporary and contract workers, agency and partner organisations aware of this Acceptable Use Policy
- educate employees, consultants, temporary and contract workers, agency and partner organisations in matters relating to Acceptable Use
- take swift and effective action within existing disciplinary and/or legislative frameworks against anyone found to be misusing the Trusts' Information Systems.

3.5 Disciplinary Procedures:

Where misuse of the Trusts' Information Systems has been identified, the matter must be the subject of investigation in accordance with the appropriate disciplinary procedure and/or legislative framework. Investigations must be carried out by the appropriate designated manager.

3.6 User Traceability:

In all cases where there is the potential for the Trust's Information Systems to have been misused, arrangements must be in place to record the identity of the individual using the specific facility at any given time and any relevant materials.

These records must be retained for the duration of the investigation and any procedures against an individual. They must also be made available to the appropriate authorities for the purposes of investigating complaints of misuse and retained for the appropriate duration as determined by the outcome. Where it is shown that there is no case to answer, the records shall be destroyed immediately.

3.7 Libel:

Libel is a civil wrong, which in proven cases may incur substantial compensation. It is very complicated and therefore one of the easiest laws to contravene through ignorance. Facts concerning individuals or organisations must be accurate and verifiable, and views or opinions must not portray their subjects in any way that could damage their reputation. Check with Information Governance if in doubt. Web pages, email messages and messages posted on discussion forums or social networks, e.g. Facebook, You Tube and Twitter, are regarded as published material – please refer to the Trusts' policies on the use of Social Networking

4. TRAINING AND SUPPORT

In order to ensure the correct implementation of this policy all managers are required to ensure that all their staff are aware and have understood its content as part of the sign off process when approving user registration applications.

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 process for monitoring compliance with the effectiveness of this policy is as follows:

Monitoring/audit arrangements	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Information & Cyber Security Audit – Spot Checks	Conduct a physical inspection of IT assets to ensure data quality within the Trust's Configuration Management Database Tool (Alloy navigator). Identify and remedy poor practice and provide ad hoc information security advice to staff. Recover any IT assets no longer required.	Information Security Manager	Joint Information Governance Board	Quarterly
Information Governance Audit – Spot Checks	IG staff members visit a service / team selected by the IG Compliance Manager, these are selected either from the incident trends identified or from a request that the service would be included within an audit.	IG Compliance Manager	Joint Information Governance Board	Quarterly

Monitoring/audit arrangements	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
	Some of the visits will be unexpected and the IG team will arrive on site and review the department/teams IG compliance. The summary findings will be compiled into a report template and this will be sent back to the team manager. Any themes will be collated and reviewed by the IG team and actions put in place to rectify ongoing themes.			

Wherever the above monitoring has identified deficiencies, the following must be in place:

- 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

6. REFERENCES:

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

Regulation of Investigatory Powers Act 2000 (RIPA)
http://www.legislation.gov.uk/ukpga/2000/23/contents

Employment Practices Code
http://ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx

7. 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.

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 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.

8.2 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 & Cyber Security Acceptable Use Policy 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

8.3 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

8.4 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.

8.5 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, that may breach acceptable use, to the JIGB.

8.6 Trust Information Security Managers’ Responsibilities

The Trust Information 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

8.7 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.

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.

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

8.8 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.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
AUP	Acceptable Use Policy
ICO	Information Commissioner's Office
ICT	Information Communication Technology
IG	Information Governance
IM&T	Information Management & Technology
IT	Information Technology
JIGB	Joint Information Governance Board
SIRO	Senior Information Risk Owner

TERM USED	DEFINITION
Blogs	Discussion or informational site published on the World Wide Web and consisting of discrete entries
CoIN	Community of Interest Network which represents the local NHS network in Cumbria
Data communications	Networks and systems used to process, store and move electronic data
Endpoint	An electronic device used by a member of staff to access information.
Malware	Software intended to do damage, deny access to disable computers and computer systems
Non-data communications	Information passed using non electronic means, e.g. voice and written documents
Social Media	Websites and applications that enable people to create and share content thereby participating in electronic social interaction
Wearable technology	Devices worn on the body to elicit physical statistics. Wearables can also enable access to information via a network

APPENDIX 1 – TABLE OF PROHIBITED USE CASES

No.	Example
1	Deliberately undertaking activities in contravention of applicable laws or regulations
2	Introducing and/or transmitting into the Trust’s Information Systems any software (including, but not limited to, computer viruses, Trojan horses and worms) designed to be destructive to the correct functioning of computer systems, software, networks and data storage, or attempting to circumvent any precautions taken or prescribed to prevent this
3	Allowing the Trust’s Information Systems to be damaged or contaminated by mishandling, food, drink, or smoking materials
4	Installing any software on any of the Trust’s Information Systems except by prior agreement with IT and under the terms of a support contract
5	The intentional access, creation, storage or transmission of material which the Trust may deem to be offensive, inappropriate, discriminatory, indecent or obscene
6	The intentional access, creation, storage or transmission of material likely to bring the Trust or its services into disrepute
7	The intentional access, creation, storage or transmission of material capable of being resolved into obscene or indecent images
8	The intentional access, creation, storage or transmission of material (other than in the course of its operations where this aspect of the business has the explicit approval of the Trust's official processes for dealing with extraordinary ethical issues) likely to cause offence, annoyance, inconvenience or needless anxiety to another or to send threatening, defamatory, discriminatory, abusive, obscene or otherwise offensive messages
9	The intentional access, storage or transmission of material, including software, films, television programmes, music, electronic documents and books which infringe the copyright of another person except where explicit permission has been given and can be evidenced
10	The creation, storage or transmission of material that breaches confidentiality undertakings in a manner which interferes with those activities covered within the definition of Acceptable Use
11	The intentional access, creation, storage or transmission of material for personal commercial gain, except where previously ratified by Trusts for the purposes of delivering private medical care
12	Attempting to gain deliberate access to facilities or services which they are unauthorised to access
13	Deliberately undertaking activities that would otherwise act against the aims and purposes of the Trust as specified in its governing documents or in rules, regulations and procedures
14	Deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users; waste employee effort or networked resources
15	Excessive use of the Internet on non-work related matters

16	Deliberately causing any of the Trust’s Information Systems to be overloaded, impaired, disrupted, curtailed or denied
17	Making commitments via email or the Internet on behalf of the Trust without full authority
18	Falsifying e mails to make them appear to have originated from someone else
19	Deliberately undertaking any activities detrimental to the reputation or business interests of the Trust
20	Deliberately contributing to News Groups, Chat Rooms or other Social Media & Networking web sites that advocate illegal or undesirable activity or is in contravention of Trust standards
21	Deliberately contributing to Social Media & Networking web sites with derogatory comments or information concerning patients or staff in contravention of Trust standards
22	Copying any material to any portable device with the intention of unauthorized disclosure
23	The intentional provision of access to unauthorized persons and/or the intentional use of another user’s credentials.
24	Intentionally taking photographs or video recordings in areas where this is expressly forbidden and failing to abide by Trust Policy on photography and video
25	Failing to lock an unattended computer or other smart device (using the Ctrl-Alt-Delete function or other applicable methods)

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
CPFT Acceptable Use Policy 002/037	v1.05	Feb2016	March 2019	Feb2016	-
NCUH Cyber Security Acceptable Use IG19	v3	8/8/2018	31/8/2021	10/8/2018	-

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1 Draft	March 2018	• Both Trust Acceptable Use policies combined into new joint template • This Policy will replace both when published
0.2 Draft	August 2018	• Content moved into new joint template • Amended Accountable Director to reflect post rather than incumbent • Added GDPR paragraph to Policy Details • Amended Table of Prohibited Action in Appendix 1 • Amended Responsibilities section to reflect current posts • Amended JIGB reporting to quarterly based on stakeholder comment • Amended Prohibited Use Case 4 to reflect software updates from external sources based on stakeholder comment
0.2 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

Name	Job Title	Date
Graham Putnam	Associate Medical Director/Chief Clinical Information Officer	17/08/2018
Dave Dagnan	Consultant Clinical Psychologist	17/08/2018
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