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

Policy Title: Joint Network Cyber Security Policy

Reference	POL/IG/010
Version	1.0
Date Ratified	19/03/2019
Next Review Date	31/03/2022
Accountable Director	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)
Policy Author	Trust Information and Cyber Security Officer

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

It is the policy of the Trusts to manage and maintain their information and information processing facilities under the aegis of a Network Cyber Security Policy as part of an Information Security Management System (ISMS) using the framework outlined in the International Standard ISO/IEC 27001:2013. The ISMS is the mechanism for ensuring that all tasks connected with Information & Cyber Security and Information Governance are drawn together in a mutually supportive way.

This policy and the policies associated with this document provide a clear statement of the Trusts' commitment to protect all physical and cyber information assets from threats internal and external, intentional or accidental.

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. All staff members must understand the requirements placed on them to keep their IT equipment safe and in operational condition.
2. All desktop and laptop computers must be connected to the network. Where roaming users are using laptops off site the laptop must be connected to the network for at least one day in every 30 days to ensure it is updated with anti-virus signatures and Windows Updates. Failure to do so will result in the laptop being excluded from the network thereby rendering it unusable.
3. Where required all relevant devices must be encrypted using the Trusts' incumbent McAfee Endpoint Security solution.
4. Smaller hand-held equipment such as Smartphones and iPads must be especially protected from loss or damage as well as inappropriate use.
5. Any attempt to breach security on a Trust device will result in disciplinary proceedings.
6. Users are not permitted to attach any personal devices to the network for the purposes of information transfer.
7. With the exception of training and educational requirements users are not permitted to process any work based information on a personal device.

TABLE OF CONTENTS

1. INTRODUCTION

This Joint Network Security Policy is a key component of the overall Information Security Management System (ISMS) framework and should be considered alongside more detailed Information & Cyber Security documentation. Appropriate documentation is now mandated by the Data Security and Protection Toolkit. Further information on the toolkit may be found at this link https://www.dsptoolkit.nhs.uk/

This Joint Policy shall cover both Trusts, including all business processes, offices (including homeworking locations), assets and technology and no exclusions shall apply unless by prior agreement.

The Trusts attach great importance to the security of their physical assets, their information processing systems and the information that they contain.

2. PURPOSE

The purpose of this Joint Policy is to detail the means by which the Trusts will achieve the required assurance levels with regard to the confidentiality, integrity and availability of all of the information assets within the Trusts' areas of responsibility. The objectives and principles of this Joint Policy also underpin the Trusts' approach to Information Governance and information sharing.

3. POLICY DETAILS

3.1 General

It is the policy of both Trusts to ensure networks are appropriately managed, protected and controlled in order that information that resides on or flows within the supporting infrastructure is protected from threats. It is also Trusts' policy to ensure that the IT Department maintains the security of the systems and applications and any information in transit to external agencies.

Both Trusts provide a data communications network facility across their major sites and other smaller sites in Cumbria. The network is mainly provided via the Cumbria Wide BT - N3 Community of Interest Network (CoIN). The network is protected by firewalls installed at all egress/ingress points.

The network provides access to both primary clinical applications such as Silverlink PAS, ORMIS, RiO, Strata, EMISWeb, PACS/CRIS, access to the Internet and to associated office services applications such as word processing, spread-sheets and email.

3.2 Access Control incl. Public Wi-Fi

To request access to the corporate network and any other Trust based information processing facilities a formal process will be used via a User Registration and De-registration Form (NCUH) or an intelligent Alloy Navigator form (CPFT).

Each user accessing this network will have an individual Active Directory (AD) User Account which will be password controlled. All User accounts will be set up by the IT Department both as part of the recruitment process and/or upon receipt of the written request, mentioned above and duly authorised by the requestor's supervisor.

Each request for user access will take into account the required security access levels, authorisation and the strict application of the 'need to know' principle. To enable the segregation of duties and to enhance security, simultaneous and totally unrestricted access to all of the Trusts' electronic information will not be permitted to any one member of staff at any time.

Accounts for personnel not employed by the Trust will be created on an 'as required' basis. For those personnel requesting network access as part of a Trust wide service delivery contract, said contract must contain a specific codicil that binds the external organisation's employees to the Trusts' Policies. Where network access is requested for other purposes the requesting individual must sign a Trust honorary contract, also to bind them to Trusts' Policies.

Generic accounts are permitted only for the purpose of providing a generic, functional mailbox, e.g. *information@department*. Generic account login details are not to be released to users.

Each user ID will be in a standard *firstname*.*lastname* format and will be created with a generic password. Users will be forced to set their own password on first logon to the network. All network passwords have a limited life-span with a change forced by the system. The system remembers that last ten (10) passwords used to prevent repetition. Unless operationally required, users should not be permitted to logon to more than one machine at a time.

Network passwords must be a minimum of eight (8) characters long and contain three (3) of the following characteristics:

- English UPPER case letters (A to Z)
- English lower case letters (a to z)
- Base 10 digits (0 to 10)
- Non alphabetic characters, e.g. !, £, $, %, &, #

As stated above, the system will remember the last ten (10) passwords used and will prevent their re-use. Passwords will last for sixty (60) days at which point the system will force users to change them.

Users of certain specialist applications will have a personal Application ID and password, which will conform, where possible, to the same rules as for an AD Account.

Public Wi-Fi access is provided by NHS Digital's 'NHS Wi-Fi' system. It is available for use nationally at all NHS sites. Staff members may also use this system but they remain bound by Trusts' Policies, in particular the Joint Cyber Security Acceptable Use Policy (AUP).

3.3 Data Centres, Servers, Network Equipment and Perimeter Controls:

All servers, physical or virtual, must be kept in an appropriately designed and correctly sized enclosure within an appropriately specified data centre. There must be a regulated power supply that is delivered via an Uninterruptable Power Supply (UPS) solution with automated management reporting built in. Enclosure based power distribution units must be of the standard appropriate to the type and size of enclosure used. The UPS must comply with relevant British and European standards.

To prevent loss of systems during a power outage all data centres must be served by an automated standby generator of sufficient capacity and power characteristics to maintain systems until the power loss incident is resolved. This generator must be tested periodically and a report submitted to the IT Department.

As part of the design and operation of the data centres full climate control must be fitted and operational. Where possible, hot and cold aisle containment should be in place with fully automated Heating, Ventilation and Air Conditioning (HVAC) monitoring systems and alarms.

All network equipment will be kept in a secure location and access to it will be restricted to members of the IT Department or any other party authorised by them. Where appropriate, support agreements will be entered into with third parties and disaster recovery plans will be produced. Support access by third parties should be via N3 where possible. Non N3 access will be by secure means and by appointment only.

Third Party Accounts will be held in a disabled state when not in use. Where a secure link is used by a Third Party, for remote access support purposes, it must be physically disabled when not in use. Access levels will be agreed with Third Parties as part of any support contract.

When access is required by the Third Party the IT Department is to be contacted for the secure link to be enabled. A log must be kept of who accessed the system, at what time, for how long, and for what purpose, this log may be held electronically. When the task is complete the secure link must be disabled once again.

Network perimeter controls are in place to ensure that all inbound and outbound traffic is authorised and is routed to its correct destination.

3.4 End User Equipment incl. Remote Support:

Users of any computing devices must comply with all current legislation and local policy that relates to the use and retention of Personally Identifiable Data and the use of computer systems.

Failure to do so may lead to withdrawal of access to information systems and devices, and would be considered for disciplinary action. Where violation of these conditions is illegal and/or unlawful, the matter may lead to prosecution.

Users of Trust owned computing devices are allocated standard user rights appropriate to their role and requirements. This is to reduce the risk of malware infection. Trust software requiring elevated rights to function is enabled seamlessly in the background on your machine, therefore not impacting your ability to do your job. If an issue is encountered, you should request support through the IT Service Desk.

Where it is impractical for an IT Technician to attend your work area such support may be carried out remotely. The ability to support a device remotely benefits the Trusts by speeding up the time taken to resolve issues, problems or queries by often eliminating the need for an engineer to visit the device.

Being able to view information on the screen and obtain details of error messages or functionality issues is critical to providing a fast resolution to many issues. Remote support can also, where appropriate, be used to provide training or guided instruction and can help to get to the root of a reported issue.

Appropriate use would be for resolving simple issues such as a user being unable to use a particular function. It is not an appropriate solution for full training on a product. Remote support is also used on many devices including Desktops, Laptops, Servers, Switches, Tablets and Smartphones.

Only those members of staff, or third parties, who have been authorised to remotely access devices may connect or attempt to connect using remote access tools. Remote support software must only to be used for diagnosis/resolution of issues and addressing simple queries with software functionality.

All remote support sessions to a device where a user is currently logged in must be approved by the user. They must be informed that you will be viewing their screen before the connection is made and asked to close any confidential information before the connection is made. Connections must only be made once explicit consent has been given and a Service Desk support ticket must exist or be created. Connection activity must be recorded against the support ticket.

Ownership of equipment and software supplied by the Trusts and used on the Trusts' network remains with the Trusts where the user is employed at all times.

Users are not to arbitrarily move or redistribute IT equipment or software. Any office move or requirement for the reallocation of IT equipment must be carried out in conjunction with the IT Department and under the control of a Service Desk request.

Mobile computing equipment and in certain areas all desktop equipment will be encrypted in accordance with the Trusts' Joint Encryption Policy. Any computer equipment not belonging to the Trusts must not be connected to the network or any other Trust owned equipment for the purpose of information transfer. This includes connection via Bluetooth, Wireless Access Point (WAP), Infrared, USB or other means. These devices are a security risk to the network.

Any exceptions must be subject to formal approval by the Trusts' Information Security Manager and subject to a full risk assessment. This includes any software not belonging to the Trust which must not be installed on Trust owned devices.

Unauthorised equipment, discovered as part of an audit or routine Service Desk call, will be immediately removed and the owner may be subject to disciplinary action.

3.5 Network Connected Medical Devices:

Medical equipment is manufactured and sold on a global basis. Many of the vendor organisations operate in many countries and, on occasion, across national boundaries. When a new system is acquired, a new support agreement is taken out for an existing system, or an emergency system failure occurs there is a chance that the vendor will offer direct technical support from their own premises. This is not normally an issue as long as the technical and procedural security systems are in place.

Any Medical Device that is connected to the Trust network via a cable or by wireless technology must, where possible, comply with the security standards within this document. Medical Engineering and IT must work together to ensure this. In each case if Patient Identifiable Data (PID) is held on any device Information Governance and Cyber Security conditions must be applied. Overall management of Medical Devices must remain with the Medical Engineering Department with the IT Department acting in a supporting role.

When a device becomes end-of-life and is marked for disposal or is being sold or traded either directly or via a third party, the on-board Residual Patient Data (RPD) must be purged. This can be carried out on site or at a specialist vendor's premises. In each case a data removal and handover (or destruction) certificate must be produced.

In the event of a device being moved to a specialist site for treatment additional conditions apply. The specialist vendor must supply information on what they do (the manual), the order in which it is done (the process map), the tools and techniques used for data erasure (by name and version), the applicable standards observed and test results from the post procedure assurance mechanism, e.g. a sample report.

Also for the above case there must be an audit of the transport security, site security and personnel security to ensure they are aware of their duties under Data Protection Act conditions. All of this is subject to periodic IG Confidentiality Audits.

3.6 Tablets, Smartphones and other Handheld Devices:

The Trusts use smartphones from several manufacturers. They also use Apple iPads, both wi-fi and wi-fi/3G. There are a number of generic mobile phones in use across the Trust. Users hold personal responsibility for the safety and security of all devices issued to them. These devices are used to make phone calls and to access the Trusts' email systems. As a result they must be incorporated into the Trusts' Mobile Device Management (MDM) system in order that corporate data can be removed or they can be completely wiped if compromised, lost or stolen.

3.7 Memory Sticks/Flash Drives:

Although in general it is not permitted to store Personally Identifiable Data (PID) on any portable device there may be exceptions when there is no other reasonable way of doing this. If this mechanism is used to transfer PID it must be deleted once the transfer is complete. Encrypted memory sticks are available from IT.

3.8 Monitoring Electronic Communications:

The Trusts provide electronic communication services (e.g. e-mail and associated functions) to staff, to enable them to communicate effectively and efficiently with other members of staff, other Trusts and partner organisations with whom they deal in the course of their normal working duties.

Network administrators will not routinely monitor all modes of communications and will take reasonable precautions to protect privacy. However, under UK Law, employers are generally liable for what their employees do in the course of their employment. This is known as vicarious liability. For this reason the Trusts' email systems incorporate profanity and other filters.

Some modes of communications, e.g. Internet access, will be subject to systematic monitoring as a matter of routine and others, e.g. email, will be subject to occasional monitoring as a short-term measure in response to a particular problem or need.

3.9 Anti-Malware & Data Loss Prevention:

Computers, tablets and Phones can be vulnerable to malicious code such as Viruses, Trojans, Worms and Spyware which can infect a PC and cause a number of undesired outcomes such as:

- Damage to equipment
- Theft/loss of information
- Reduction in performance
- Financial theft

All devices need protection from this type of threat through the use of a number of tools including Antivirus software and Software patching.

Malicious Software, known as malware, can spread in a number of ways including:

- Self-replication across the network
- Intentional or unintentional installation by users
- Installation through infected devices (e.g. USB sticks)
- Automatically scripted installation
- Exploitation of vulnerabilities

Often malware exploits existing vulnerabilities in software in order to infect a device. Software manufacturers issue patches that can be installed to remove the vulnerability and reduce the likelihood of infection.

Deployment of Data Loss Prevention (DLP) is intended to prevent the unauthorised extraction of data to personal memory sticks and external disks. It will have a default setting of device lock down, read from all, write to approved only. Managers will be expected to identify devices where there is a business need to exclude them from this control. Exclusions will require a risk assessment of the device identified and will be recorded in the Trust's Service desk system. Port Control is part of the overall Data Loss Prevention mechanism.

The solution used for both anti-malware and DLP is the McAfee Endpoint Security suite. Further information can be found in the Joint Encryption Policy.

3.10 Secure Disposal:

The Trust holds and processes large amounts of information including personal sensitive information. The Data Protection Act (2018) requires that this information is processed securely, using appropriate technical or organisational measures, and disposed of correctly when no longer required. As information can remain on Hard Disks and other media it is vital that this equipment is destroyed in a safe and secure way to avoid data being recovered by unauthorised persons.

Alongside the security implications the Trusts are also required by law to comply with the Waste Electric and Electronic Equipment (WEEE) Regulations 2013, which covers the recovery, reuse, recycling and treatment of electrical waste.

All data held on IT equipment shall be assumed to contain Special Category Data, as defined in Article 9 of the GDPR, e.g. health, race or union membership. This data is to be stored and handled in a manner appropriate to this classification of data. Only physical destruction of all data is acceptable. Remote wiping techniques are not to be used except to provide additional assurance prior to physical destruction.

Where disposal is undertaken by a third party, a certificate of destruction must be provided for each item of equipment. This must detail the process used to destroy the data. Where the Trust is leasing equipment, staff responsible for the contracts must ensure that the contract certifies the destruction of data held on the devices during the period of the lease.

Where data is held "online" or "In the cloud" such as in a hosted data centre, staff responsible for the contracts must ensure the contract certifies the destruction of data held either when the data is no longer required or at the end of the contract once the data has been passed back to the Trust.

Any media, covered as part of a maintenance contract, such as Server hard disks, must have a media retention clause in the contract stipulating that faulty equipment must not be returned to the supplier as it could contain sensitive data. Where a media retention contract does not exist, any faulty equipment must be kept on site and paid for if necessary. It must then be destroyed.

3.11 Change Management:

The primary objective of change management is to enable beneficial changes to be made, with minimal disruption to IT services. Change Management, via the Change Advisory Board (CAB), ensures that changes are deployed in a controlled way, i.e. they are evaluated, prioritised, planned, tested, implemented and documented and the impact of the change is fully understood.

Changes can be made for proactive or reactive reasons. Proactive reasons could include patching software, reducing costs, improving or introducing new services. Reactive reasons could include resolving issues that are occurring. Rigorous change management processes are fundamental in the delivery of a reliable IT service and ensuring the stability and integrity of these services.

All changes must be authorised prior to implementation. The changes must be implemented as per the details on the approved request. The change must take place at the approved time as decided by CAB. Any deviation to this time requires approval prior to implementation. All changes must include a back out/reversion plan. Unauthorised changes are not permitted.

Emergency changes must be approved by an Emergency CAB prior to implementation. All emergency changes will be logged via the IT Service Desk in response to an identified issue managed by a specific Service Desk ticket.

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

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
On-going review of Information Security	Cumbria Cyber Security Group and	Head of IG	Joint IG Board	Quarterly

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Elements – concerns and issues highlighted to the Board.	Joint IG Board reviews			
Breach Incident Reports	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

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:

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

Computer Misuse Act 1990
http://www.legislation.gov.uk/all?title=computer%20misuse%20act

Employment Practices Code
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

7. ASSOCIATED DOCUMENTATION:

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

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

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

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 Trust, including ensuring that Trust policies comply with all legal, statutory and good practice requirements.

8.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates):

The Executive Director of Finance & Strategy is responsible for ensuring the development and sign off of this Policy. They ensure the policy is kept up to date by the relevant author and approved at the appropriate committee.

8.3 Senior Information Risk Owner (SIRO) Responsibilities:

The SIRO has responsibility for ensuring that a Mobile Computing & Remote Access 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 framework 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

The role of the SIRO:

- Is accountable for approving all Information Assets.
- Fosters a culture for protecting and using data.
- Provides a focal point for managing information risk and incidents.
- Is concerned with the management of all information assets.
- To provide a focal point for the resolution and/or discussion of information risk issue.
- Ensure that all care systems information assets have an assigned Information Asset Owner.
- Ensuring the Organisation has a plan to achieve and monitor the right Information Governance culture, across the organisation and with its business partners.
- Approval of all information asset business continuity plans.

- Document a plan for information security assurance that identifies the support necessary to ensure work related to information security management is appropriately carried out.
- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Review and agree action in respect of identified information risks.

8.4 Caldicott Guardian Responsibilities:

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

8.5 Managers/Information Asset Owner's and Administrator's Responsibilities:

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

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 continuity plans in the event of system unavailability.

IAOs are responsible for:

- Leading and fostering a culture that values, protects and uses information for the success of the organisations and benefit of their 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 SIRO.

The Information Asset Owner 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.

Managers are also responsible for ensuring adequate dissemination and implementation of policies relevant to the staff in their areas. Managers are also responsible for ensuring staff members understand how to access policies on the Intranet.

8.6 Approving Committee Responsibilities: Joint Information Governance Board

The Joint IG Board is the oversight committee for all items relating to information governance and reports into the Joint Clinical Governance Group and Quality and Safety Committee (Board Sub Committees) as required. In terms of policy responsibilities the role of the Joint IG Board is to ensure that local policies compliment the national policy, strategy and guidance relating to information governance and that it is implemented and evaluated appropriately within the Trust. The Joint IG Board are responsible that regular review of information governance policies and procedures takes place and monitors policy compliance at each of its meetings.

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.

8.7 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

8.8 Trusts' Joint IT Department's Responsibilities

To maintain good Cyber Security practice the IT Departments are required to hold responsibility for certain aspects of the overall network infrastructure.

Data available to IT Department support staff will always be treated as confidential and will not be disclosed, modified or replicated without the express permission of the Caldicott Guardian, Head of Information Governance, or the owner of the data.

Controls are in place governing the way members of the support staff connect to workstations to commence technical support. Standard Operating Procedures must be in place to support all aspects of this Joint Policy.

With regards to the network servers and data communications equipment, IT holds but is not limited to, the following responsibilities:

- Specification and purchase of all new equipment
- Monitoring the availability of the servers/network when in use
- Ensuring the correct software level is maintained and any upgrades that may be required are implemented in a controlled manner

[1] Such as the NHS Digital CareCERT Information sharing Portal
https://nww.carecertisp.digital.nhs.uk/display/CC/CareCERT+Information+Sharing+Portal+Home

- Arranging and managing hardware support agreements
- Administration and maintenance of all perimeter controls, e.g. firewall(s), email content filters, proxy servers and anti-malware/anti-phishing services
- Maintaining a data backup mechanism, including storage and replacement of media
- Ensuring that Anti-Malware software is installed and maintained on all machines
- Web monitoring
- Trouble-shooting both hardware and software operational problems
- Safe and secure disposal of equipment

With regards to desktop and mobile computers IT is responsible for:

- Specification of new machines
- Configuration of each PC to the agreed standard build, including full-disk encryption where necessary
- Loading additional software on the PC
- Device Control/Data Loss Prevention
- Removing any unauthorised software from the PC
- Trouble-shooting both hardware and software operational problems
- Provision of local admin level access in exceptional cases
- Safe and secure disposal of equipment

With regards to the Network administration, IT is responsible for:

- Management and maintenance of all servers and networking equipment
- Ensuring unused network ports are disabled
- Maintenance of domain administrator logon IDs and passwords
- Creation, removal and maintenance of all AD Accounts
- Periodic audit of the user accounts
- Maintenance of the Email Global Address Book

8.9 Staff Responsibilities:

All staff members are responsible for co-operating with the development and implementation of Trust policies as part of their normal duties and responsibilities. They are responsible for ensuring that they maintain up to date awareness of corporate and local policies with regard to their own and their staff roles and responsibilities.

In addition each user is required to abide by the terms of the Information Security Acceptable Use Policy. Users are also responsible for the appropriate use and operation of the equipment they are using in their work. They must ensure that they comply with and are able to reference all relevant policies, standards and guidance and they understand good practice in terms of Information Security and Health & Safety requirements.

These standards include but are not limited to:

- Ensuring their password is kept confidential
- Changing their password if a breach of security is suspected
- Reporting any known or suspected breach of security
- Not allowing another user to login on their ID
- Not using another user's ID to login
- Not loading any additional software onto the PC
- Not amending the configuration settings of the PC
- Maintaining the confidentiality of data in their care
- General housekeeping of their data on the networked drives
- General housekeeping of the content of their email box

9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
AD	Active Directory
AUP	Acceptable Use Policy
BT-N3	National NHS Network
CoIN	Community of Interest Network
CRIS	Computerised Radiology Information System
DLP	Data Loss Prevention
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ISMS	Information Security Management System
ISO/IEC	International Standards Organisation/International Electrotechnical Commission
ORMIS	Operating Room Management Information System
PACS	Picture Archiving and Communications System
PAS	Patient Administration System
PID	Patient/Personally Identifiable Data
SIRO	Senior Information Risk Owner
UPS	Uninterruptable Power Supply
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Access Point
Wi-fi	Wireless Fidelity

TERM USED	DEFINITION
256 bit AES	Advanced Encryption Standard – is the technology used to hide (encrypt) or unhide (decrypt) data. It uses a 256 bit key length.
7Zip	Open source archiving software which is included in the current Trusts' PC Build.

TERM USED	DEFINITION
Availability	The system or device being accessible and usable on demand.
Bluetooth	A standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
Caldicott Guardian	Designated senior medical officer to oversee all procedures affecting access to person-identifiable health data.
Confidentiality	Information / data is not made available or disclosed to unauthorised individuals, entities or processes.
Decryption	The process where an encrypted file/device is made readable using a password or key.
Encryption	The process where a readable file/device is made unreadable.
Integrity	Process of safeguarding the accuracy and completeness of assets, such as information and data.
Internet Filter	A device that examines Internet connection requests to determine if they are permitted.
McAfee Endpoint Security	Encryption and Data Loss Prevention tool used by the Trusts to protect data on portable devices. Often called ‘Drive Encryption’ and ‘Port Control’.
Mitigation	Used to limit the negative consequences of a risk / particular event.
Password / Key	A word or string of characters when entered alongside a username to log in, or to gain access to some resource i.e. a laptop or desktop. Passwords / keys are a common form of authentication.
PID	Personally Identifiable Data such as patient and staff demographics.
Port Control	A mechanism for enabling or ‘locking down’ communications ports on network attached devices.
Proxy Server	A server that offers a service allowing a user to make indirect connections with other networks.
Risk	Is an uncertain event(s) which should it occur will have an effect on objectives.

TERM USED	DEFINITION
Risk Assessment	Overall process of risk analysis and risk evaluation.
Self-decrypting	Where a file/device is made readable again without visible intervention such as the input of a password or key.
Self-extracting	Is a computer application which contains a compressed file archive, as well as programming to extract this information held within the file.
Sensitive Data	Information / data that is confidential and for senior managers only such as financial and management.
Single Sign On	Is a method of access to a device that enables a user to log in once and gain access to the device and systems without being prompted to log in again.
Vicarious Liability	Refers to a situation where someone is held responsible for the actions or omissions of another person. In a workplace context, an employer can be **liable** for the acts or omissions of its employees, provided it can be shown that they took place in the course of their employment.
Windows Active Directory	Active Directory allows administrators to assign policies, deploy software, and apply critical updates to an organisation's information processing assets. Active Directory stores information and settings in a central database.
Windows Update	An automated mechanism for applying updates and security patches to Windows operating systems on computers

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	Joint IG Board 15/03/2019

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published
NCUH IG28 Network Cyber Security Policy v1.0	17/11/2016	Nov 2019	14/12/2016
CPFT POL/002/002 Access Control	10/2/2016	Mar 2019	Feb 2016

Version	Ratified Date	Review Date	Date Published
VFeb16			
CPFT POL/077/006 Anti-malware vFeb16	10/2/2016	Mar 2019	Feb 2016
CPFT POL/002/007 IT Equipment Secure Disposal V Aug16	31/8/2016	Mar 2019	Sep 2016
CPFT POL/002/008 eHealth Change Management vMay16	May 2016	Mar 2019	May 2016
CPFT POL/002/010 Remote Support End Users Device vMay 16	1/5/2016	Mar 2019	Oct 2016

Statement of changes made from previous versions: CPFT and NCUH policies

Version	Date	Section & Description of change
0.1 Draft	March 2018	• New policy in new joint template
0.2 Draft	19/01/2019	• Whole document amended to reflect peer review comments • Training section updated • References section update • Associated Documentation section updated • Stakeholder list updated • Sections added covering access control, secure disposals and change management • Abbreviations and Definitions updated •
0.2 Draft	25/01/2019	• Stakeholder amendments added for typos and syntax where applicable
0.3 draft	12/03/2019	• Reference to previous trust policies in Doc Control section
0.4 draft	19/03/2019	Minor amendments following Policy Management Group meeting: • Added Joint IG Board approval date to Policy front page and document control section, and Policy Checklist • Section 8.5 Joint IG Board Responsibilities - added clarification that this is the approving committee for the Policy. • Section 1 Introduction (page 4) replaced Wikipedia definition with industry standard reference. • Section 1 Introduction replaced hyperlink “here” with the web address • Removal of “network security” definition from Section 1 Introduction

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	10/01/2019
Robin Andrews	Interim Executive Director of Finance	10/01/2019
Andrew Brittlebank	Medical Director	10/01/2019
Graham Putnam	Associate Medical Director/Chief Clinical Information Officer	10/01/2019
Dave Dagnan	Consultant Clinical Psychologist	10/01/2019
Farouq Din	Associate Director of Digital Health	10/01/2019
Daniel Scheffer	Associate Director for Corporate Governance/Company Secretary	10/01/2019
Lesley Paterson	Associate Director of Quality & Nursing (Specialist Services)	10/01/2019

Name	Job Title	Date
Lyn Moore	Associate Director of Operations	10/01/2019
Mandy Annis	Employment Services Bureau Manager	10/01/2019
Julie Thompson	Head of Workforce Services	10/01/2019
Elizabeth Klein	Head of Nursing - Clinical Standards	10/01/2019
Jacky Stockdale	Joint Business Manager - Corporate Services	10/01/2019
Paula McBride	Deputy Business Manager	10/01/2019
Kirsty Jay	Deputy Business Manager	10/01/2019
Laura Parkinson	Head of PMO	10/01/2019
Yvonne Salkeld	Head of IG	10/01/2019
Steve Johnstone	Joint Interim Head of IT	10/01/2019
Sarah Sproat	Clinical Nurse Specialist in Palliative Care	10/01/2019
Lorraine Gray	Head of Information	10/01/2019
Natalie Karam	Head of Performance	10/01/2019
David Franklin	Financial Systems Manager	10/01/2019
Kath Watts	Network Manager - First Step	10/01/2019
Katherine McGleenan	Clinical Quality Manager	10/01/2019
Anne Gadsden	Information Governance Officer	10/01/2019
Paul Corrie	Information Governance Compliance Manager	10/01/2019
All NCUH Business Managers		10/01/2019