Outstanding Care,
Compassionate People,
Healthier Communities

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

ACCEPTABLE USE OF THE NETWORK POLICY

<table>
<tr><td colspan="3"></td><td><b>POLICY</b></td></tr>
<tr><td><b>Reference</b></td><td colspan="3">IG/009</td></tr>
<tr><td><b>Approving Body</b></td><td colspan="3">Cyber Security Assurance Programme Board</td></tr>
<tr><td><b>Date Approved</b></td><td colspan="3">23rd July 2024</td></tr>
<tr><td rowspan="3"><b>For publication to external SFH website</b></td><td colspan="3"><b>Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:</b></td></tr>
<tr><td><b>YES</b></td><td><b>NO</b></td><td><b>N/A</b></td></tr>
<tr><td>x</td><td></td><td></td></tr>
<tr><td><b>Issue Date</b></td><td colspan="3">23rd July 2024</td></tr>
<tr><td><b>Version</b></td><td colspan="3">4</td></tr>
<tr><td><b>Summary of Changes from Previous Version</b></td><td colspan="3">Review- minor changes and updates to formatting
Addition of policy development process at section (2) and references to Cyber Security Assurance Programme Board approval.</td></tr>
<tr><td><b>Supersedes</b></td><td colspan="3">3</td></tr>
<tr><td><b>Document Category</b></td><td colspan="3">Information Governance</td></tr>
<tr><td><b>Consultation Undertaken</b></td><td colspan="3">Cyber Security Assurance Programme - Delivery Group
IG Working Group</td></tr>
<tr><td><b>Date of Completion of Equality Impact Assessment</b></td><td colspan="3">5th June 2024.</td></tr>
<tr><td><b>Date of Environmental Impact Assessment (if applicable)</b></td><td colspan="3">Not applicable.</td></tr>
<tr><td><b>Legal and/or Accreditation Implications</b></td><td colspan="3">Data Protection Act 2018
UK General Data Protection Regulation
NIS Regulation</td></tr>
<tr><td><b>Target Audience</b></td><td colspan="3">All staff</td></tr>
<tr><td><b>Review Date</b></td><td colspan="3">2 years – 23rd July 2026</td></tr>
<tr><td><b>Sponsor (Position)</b></td><td colspan="3">Cyber Security Assurance Programme - Chair</td></tr>
<tr><td><b>Author (Position &amp; Name)</b></td><td colspan="3">Cyber Security Assurance Delivery Group members</td></tr>
<tr><td><b>Lead Division/ Directorate</b></td><td colspan="3">Corporate</td></tr>
<tr><td><b>Lead Specialty/ Service/ Department</b></td><td colspan="3">Information Security - Information Governance</td></tr>
<tr><td><b>Position of Person able to provide Further Guidance/Information</b></td><td colspan="3">Cyber Security Assurance Programme Delivery Group</td></tr>
<tr><td colspan="2"><b>Associated Documents/ Information</b></td><td colspan="2"><b>Date Associated Documents/ Information was reviewed</b></td></tr>
<tr><td colspan="2">1. Network Security Policy
2. Information Security Policy</td><td colspan="2">June 2022
April 2023</td></tr>
<tr><td colspan="2">Template control</td><td colspan="2">June 2020</td></tr>
</table>

CONTENTS

APPENDICIES

1.0 INTRODUCTION

This policy applies to the acceptable use of NHS systems, devices or applications deployed in support of NHS or health and social care business functions and provided by Nottinghamshire Health Informatics Service (NHIS). This is to ensure that the applicable and relevant security controls are set in place in line with the Department for Health, the wider NHS, health and social care and UK Government requirements as set by the National Cyber Security Centre (NCSC).

Nottinghamshire Health Informatics Service (NHIS) policy is to ensure that hardware and software utilised by partners and customer end users is as secure as possible. As a general principle, the network and provided IT systems **shall** be locked down as much as possible without inhibiting business requirements or affecting the availability of clinical information systems.

If hardware and software (operating systems and programmes/applications) are not securely configured the number of potential vulnerabilities is increased and this makes the systems more at risk of not only being attacked but exploited with data breaches, loss of service and reputational damage the result. Guidance from NHS Digital states that every organisation should aim to either have, or contractually require, its IT systems configured as securely as possible.

2.0 POLICY STATEMENT

This document has been developed as part of the Nottinghamshire Health Informatics Service (NHIS) and partner commitments to maintaining a secure network as part of the Cyber Security Assurance Programme.

The Policy has been reviewed and developed by:

- Nottingham and Nottinghamshire Integrated Care Board
- Sherwood Forest Hospitals NHS Foundation Trust
- Nottingham CityCare Partnership

All partners are committing to the principles of the policy and protection of the shared network through management of user access. The Trust will ensure that users understand their responsibilities regarding use of the shared network.

This document is aligned to the NHS Digital exemplar materials and in line with NHS Good Practice Guidelines and should be referenced to individual organisation Information Security Policies and Acceptable Use of the Internet and Email Policies.

This policy is aligned to the ISO 27001:2022 standard controls for use of network resources and in line with information security policies and procedures.

Control Ref	Title
A.5.1	Policies for Information Security
A.6.7	Remote Working

3.0 DEFINITIONS/ ABBREVIATIONS

Senior Information Risk Owner – SIRO
Information Asset Owner - IAO
Information Asset Administrator - IAA

4.0 ROLES AND RESPONSIBILITIES

Groups & Committees

The Cyber Security Assurance Programme (CSA) has developed these documents to further ensure the security of the shared network and infrastructure. They have been developed by the CSA Delivery Group, consulted on by each partner by their internal governance and then approved by the CSA Programme Board**.**

Trust Board

The Board has the Individual Officer arrangements in place to ensure that requirements are carried out effectively.

Information Governance (IGC) Committee

The Committee is responsible for ensuring that this policy is implemented, including:

- Providing management direction and support for removable media activities in accordance with business requirements

- Ensuring additional guidance and training deemed necessary to support removable media activities are implemented

- It will monitor and provide Board assurance in this respect.

The Committee reports to the Risk Committee.

Individual Officers

The Chief Financial Officer, in their role as Senior Information Risk Owner (SIRO) is to take ownership of the organisation's information risk and act as an advocate for information risk on the Board, assisted by the Information Governance department.

Information Asset Owner’s/ Information Asset Administrator’s will be responsible for implementing and maintaining the policy in their area of management, including ensuring that procedures are in place and staff have adequate access to information security training for their asset.

Information Asset Administrators (IAAs) have day to day responsibility for managing security aspects of their assets.

Information Asset Owners will review the security of information systems and removable media on a regular basis, and this will be subject to internal audit through incident reporting.

All members of staff should read and note the contents of this policy and must have access to and conscientiously follow the guidance outlined in their local policies and procedures.

The Caldicott Guardian will be central to the framework for handling personal confidential data in the NHS and will be fully aware of their responsibilities specified in the Caldicott Guardian Manual (Department of Health, 2017 Manual).

All staff are responsible for reducing the likelihood of actual or potential security breaches occur as a direct result of their actions.

The Trust will investigate all suspected/actual security breaches and report through their incident reporting procedures.

5.0 APPROVAL

Approval of the Policy will be through the Cyber Security Assurance Programme Board, with appropriate consultation through relevant Trust officers and the Information Governance Working Group. The Information Governance Committee will formally accept the Policy for the Trust and ensure that Trust Staff are aware of the principles of the Policy.

6.0 ACCESS CONTROLS

Access to IT systems shall be based on ‘least privilege’. This applies to administrator and user access to hardware, software (Operating systems and applications), data, network configurations and security features.

Least privilege means giving a user account only those privileges which are essential to perform its intended function; this applies to everyday users and to system and application administrators. Its aim is to enhance the protection of data and information processed and the IT/software functionality from faults and malicious behaviour, whilst facilitating safe and effective patient care. This principle applies to all personal data processing.

7.0 SECURE CONFIGURATION

NHIS controlled and managed systems and services shall be deployed to ensure that all unnecessary functionality is removed, and default configurations applied. The aim of this is to minimise the routes that an attacker could use to damage the system or obtain other confidential information. Baseline security configurations shall be developed to ensure a consistent build for all client and server systems.

Protective monitoring **shall** be in place to detect any attempt to modify the configuration of all client and server systems and client systems will be configured so that it is not possible to modify the boot configuration.

Client and server systems shall be locked down to remove, prevent or limit access to unnecessary physical and logical communications ports (e.g. USB, TCP/IP), removable media (e.g. CD/DVD drives), network communications interfaces (e.g. Infrared, Bluetooth, and Wireless).

Operating systems shall be locked down to remove or prevent access to unnecessary applications and services that are not relevant and necessary to fulfil their role.

Client and server systems shall only host the applications required to carry out the business processes.

8.0 USE OF INFORMATION SYSTEMS

Third party individuals and employees of partner and customer organisations **shall** only be authorised access to information relevant to their work and will be revoked on termination of employment.

Accessing or attempting to gain access to unauthorised information **shall** be deemed a disciplinary offence and will be dealt with under the applicable organisations disciplinary policies.

When access to information is authorised, the individual user **shall** ensure the confidentiality and integrity of the information is upheld, and to observe adequate protection of the information according to NHS policies as well as legal and statutory requirements. This includes the protection of information against access by unauthorised persons.

All staff must be made aware that they have a duty of care to prevent and report any unauthorised access to systems, information, and data.

Where an organisation has identified a business need for a system or application, outside the standard configuration or build to be connected to the network, then a formal risk assessment must be conducted to assess any potential impact on the network services provided – particularly where clinical systems are being delivered.

9.0 MISUSE OF INFORMATION SYSTEMS

Use of NHS information systems for malicious purposes **shall** be deemed a disciplinary offence. This includes but is not limited to:

Penetration attempts (“hacking” or “cracking”) of external or internal systems except for the NHIS Cyber Team who may undertake these as part of their role in maintaining the security of any network, owned, managed, or maintained by NHIS and then only with permission of Senior Cyber-Engineer or Senior Security Operations Centre (SOC)/Security Information and Event Management (SIEM) member.

Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.

Discriminatory (on the grounds of sex, political, religious, or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.

Acquisition or proliferation of pornographic or material identified as offensive or criminal.

Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software.

Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads. For advice staff should contact the NHIS Service Desk.

All staff must be made aware of what constitutes misuse and the potential consequences of any misuse of systems, information and data and must abide by their organisations information security and information governance.

Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is strictly forbidden and **shall** be deemed a disciplinary offence (Computer Misuse Act).

Access to any information, records or medical information which is not required as a specific provision of their role.

Use of NHS information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and **shall** be deemed a disciplinary offence.

If identified misuse is considered a criminal offence, criminal charges **shall** be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

10.0 GUIDELINES FOR IT EQUIPMENT USE

Physical Protection

- Users **must** not expose any IT equipment to magnetic fields which may compromise or prevent normal operation.

- Users must not expose any IT equipment to external stress, sudden impacts, excessive force, or humidity.

- Only authorised NHIS engineers **shall** be allowed to open NHS IT equipment and equipment cabinets.

- Equipment must never be left unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure.

- Equipment **must** never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures. Portable equipment **shall** be physically locked down or locked away when left in the office overnight.

- Equipment should not be checked in as hold luggage when travelling but always treated as hand or cabin luggage.

General Use

- Users **must** lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method) when left unattended, even for a short period.

- Users **must** not install unapproved or privately-owned software on NHS IT equipment.

- Only authorised NHIS IT personnel **shall** be allowed to reconfigure or change system settings on the IT equipment

Laptops and mobile devices shall:

- Only be used by the NHS or third-party employees that have signed and taken personal responsibility for the laptop.

- Have the corporate standard encryption software installed, rendering the information on the laptop inaccessible if the laptop is stolen or lost.

- Have the corporate standard anti-virus, anti-spyware and personal firewall software installed and the corporate standard remote access installed.

- When configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.

- NHS laptops **must** never be (via cable or wireless) directly connected to other non-NHS IT equipment or systems.

- Users **must** not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data.

- Any device lost or stolen **must** be reported immediately to the employees line manager, NHIS Service Desk and Information Governance team (or equivalent) and local incident reporting procedures.

Internet Acceptable Use

- Internet access via the NHS infrastructure is provided for business purposes. For simplifying everyday tasks, limited private use may be accepted. Such use includes access to web banking, public web services and phone web directories. Users should refer to their organisations acceptable use policy.

- The section below is based on UK Government and industry best practice and guidance; however, it is recognised that some organisations' working practices may mean that some elements may not be applicable. If this is the case it is highly recommended that a full security risk assessment is conducted prior to any major deviation from this guidance.

- Excessive personal use of the Internet during working hours shall not be tolerated and **may** lead to disciplinary action.

- Users **shall** not use Internet-based file sharing applications, unless explicitly approved and provided as a service.

- Users **shall** not upload and download private data (e.g. private pictures) to and from the Internet or use any NHS storage provision for personal use.

- Users must ensure they abide by organisational policy for Acceptable Use of the Internet about downloading of copyrighted material from the internet.

- Users **shall** not use NHS systems or Internet access for personal advantages such as business financial transactions or private business activities.

- Users **shall** not use their organisational identity (i.e. e-mail address) for private purposes such as on social media, discussion forums and should only be used for work purposes.

11.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (e.g verbal, formal report etc) and by who)
Regular monitoring	Head of Data Security and Privacy	Internal/external audits	Bi-monthly	Cyber Security Assurance Delivery Group/Information Governance Committee

12.0 TRAINING AND IMPLEMENTATION

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[1] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[2]

Monitoring Assessments

The process for monitoring and evaluating the effectiveness of this policy, including obtaining evidence of compliance, will be a part of the Information Governance annual audit process overseen by the Information Governance Committee.

The requirements identified in this document will be subject to regular monitoring with random audits conducted by Internal/External auditors, to ensure compliance and identified breaches/non-compliance will be dealt with accordingly.

13.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 2
- This document is not subject to an Environmental Impact Assessment

14.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- ISO27001:2017

[1] https://sfhcoursebooking.nnotts.nhs.uk/fulldetails.aspx?recid=195(internal web link)
[2] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

Related SFHFT Documents:

- Network Security Policy
- Information Security Policy
- Cyber Security Guidance
- Email and Internet Policy
- Data Protection, Confidentiality and Disclosure Policy and Procedure

15.0 KEYWORDS

Cyber security, information, integrity, availability, security, data, IT.

16.0 APPENDICES

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Acceptable Use of the Network Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 5th June 2024			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion / Belief	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None

Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None for this version, in that all previous principles remain in accordance with previous version (which was subject to consultation), and this version is primarily a reformat and codification of agreed practices.

What data or information did you use in support of this EqIA?

- Trust policy approach to availability of alternative versions.

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints, or compliments?

- No.

Level of impact

Low Level of Impact

Name of Responsible Person undertaking this assessment: NHIS Head of Corporate and Business Support

Signature: R Lloyd

Date: 5th June 2024

APPENDIX 2 – USER GUIDANCE

User Guidance

Information technology resources, such as PCs, laptops, Smart Phones and Tablet devices offer new and exciting ways of working and engaging with our colleagues and patients. However, we must also be aware that improper use can impact us, our colleagues, patients, the reputation of the NHS and the public purse.

You will only be given access to systems and information that you require to carry out your work. Accessing or attempting to gain access to systems or information for which you have no 'Need to Know' or 'Need to Use', could be deemed a disciplinary offence.

In line with your organisational policies as well as legal and statutory requirements, all individuals must always ensure that you adequately protect the confidentiality and integrity of any system or information you have been authorised access to. This includes protection against access by unauthorised persons. Further guidance can be gained from your local Security Team and your Line Manager.

Protection of Systems

Internet Acceptable Use

Internet access via the NHS infrastructure is provided for business purposes to simplify everyday tasks. Limited private use, such as access to web banking, public web services and phone web directories is accepted but excessive personal use of the Internet during working hours should be avoided.

You should not use NHS systems to access the Internet or use your NHS e-mail address for private business activities (such as eBay or auction sites), downloading software, images, music, and videos or for personal financial advantage or for private social media and discussion forums.

Work Email Acceptable Use

Email services are provided to you for business purposes. Limited private use for the purpose of simplifying everyday tasks is accepted but private emails should be distributed via web-based email services. Private emails should be stored in a separate folder named **'Private e-mail box'**. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection. Private emails should be deleted as soon as possible to limit storage requirements for non-business information.

You must not use external, web-based e-mail services (e.g. hotmail.com) for official or NHS business communications and purposes.

You must not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic, or obscene, distribute statements of a political or religious or of a personal nature or engage in any illegal activities via e-mail.