NHS
Nottingham and Nottinghamshire
Integrated Care Board

Acceptable Use of the Network Policy

July 2022 – July 2025

CONTROL RECORD				
Reference Number GOV-011	**Version** 1.0	**Status** Final	**Author** Cyber Security Assurance Programme Board	
			Sponsor Information Governance Steering Group	
			Team Information Governance Team	
Title	Acceptable Use of the Network Policy			
Amendments	None			
Purpose	The purpose of this policy is to set out the acceptable use of NHS systems, devices, applications or services deployed in support of NHS or health and social care business functions and provided by Nottinghamshire Health Informatics Service (NHIS) on behalf of the Nottingham and Nottinghamshire Integrated Care Board.			
Superseded Documents	None			
Audience	All end users such as staff, third parties, contractors and partners of systems, devices, applications or services supplied to them by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions.			
Consulted with	The Policy has been reviewed and developed by the Cyber Security Assurance (CSA) Delivery Group and approved by the CSA Programme Board.			
Equality Impact Assessment	June 2022			
Approving Body	ICB Board		**Date Approved:**	1 July 2022
Date of Issue	July 2022			
Review Date	July 2025			
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.				

NHS Nottingham and Nottinghamshire Integrated Care Board (ICB)'s policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnicb-nn.comms@nhs.net.

Contents

1. Introduction

1.1. 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) on behalf of Nottingham and Nottinghamshire Integrated Care Board (ICB). 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).

1.2. 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 or other business information systems.

1.3. 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. Purpose

2.1. This policy sets out the responsibilities of individuals that access the network and /or use devices or applications provided by NHIS on behalf of Nottingham and Nottinghamshire ICB and are deployed in support of NHS or health and social care business functions.

3. Scope

3.1. The Acceptable Use Policy applies to:

- All employees who work for or on behalf of the Nottingham and Nottinghamshire ICB including those on temporary or honorary contracts, secondments, volunteers, Integrated Care Board members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the ICB.
- All Nottingham and Nottinghamshire ICB Directors, Heads of Departments, Senior Managers nominated Information Asset Owners and Information Asset Managers are responsible for the security of their systems, devices or applications supplied to their business area by Nottingham and Nottinghamshire Integrated Care Board to support its health and social care business functions.

4. Definitions

4.1. Acceptable Use Policy definition:

Term	Definition
Acceptable Use Policy	Set of rules applied by the owner, creator or administrator of a computer network website, or service, that restricts the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

5. Roles and Responsibilities

5.1. This table sets out Acceptable Use of the Network Policy key responsibilities for specific roles and staff groups in relation to delivering the objectives of this policy.

Role	Responsibilities
Trust Board	The Board must have Individual Officer arrangements in place to ensure that requirements of this policy are carried out effectively.
Senior Information Risk Owner (SIRO)	The Chief Financial Officer, in their role as Senior Information Risk Owner (SIRO) takes ownership of the organisation's information risk and act as an advocate for information risk on the Board.
Information Governance Steering Group (IGSG)	IGSG reports to the Audit and Risk Committee and is responsible for ensuring that this policy is implemented, including: • Providing management direction and support for Acceptable Use of the Network requirements in accordance with business requirements • Ensuring additional guidance and training deemed necessary to support Acceptable Use of the Network requirements are implemented • It will monitor and provide Board assurance in this respect.
Information Asset Owner's (IAOs) / Directors	Are responsible for implementing and maintaining this policy in their area of management of Nottingham & Nottinghamshire ICB systems, devices or applications, ensuring that procedures are in place and staff have adequate access to information management and security training.

Role	Responsibilities
Designate Heads of Department and Senior Managers	Are responsible for implementing and maintaining this policy in their area of management of Nottingham & Nottinghamshire ICB systems, devices or applications ensuring that procedures are in place and staff have adequate access to information management and security training.
Information Asset Managers (IAMs) and line managers	Information Asset Managers (IAMs) have day to day responsibility for managing their information assets and associated records management, confidentiality, integrity and availability to include information security.
All Staff	All members of staff should read and note and fully adhere to the requirements of this policy and must have access to and follow the guidance outlined in related local SOPs/Processes and procedures. The ICB will investigate all suspected/actual security breaches and report through their incident reporting procedures.
Caldicott Guardian	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).

6. Acceptable Use of the Network - Controls

6.1. Access Controls

Access to IT systems shall be on the basis of '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.

6.2. 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.
- Client and server systems shall only host the applications required to carry out the business processes.

6.3. **Use of Information Systems, Applications and Devices Responsibilities**

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, integrity and availability 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 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 in order to assess any potential impact on the network services provided – particularly where clinical systems are being delivered.

6.4. **Misuse of Information Systems, Applications and Devices**

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.
- 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.
- 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).
- 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.

6.5. **IT Equipment and Mobile Devices – Physical Protection**

- Users shall not expose any IT equipment to magnetic fields which may compromise or prevent normal operation.
- Users shall 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.
- Portable equipment shall never be left unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure.
- Portable equipment shall 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.

- Portable equipment shall not be checked in as hold luggage when travelling but treated as hand or cabin luggage at all times.

6.6. **IT Equipment and Mobile Devices – General Use**

User guidance is summarised at **Appendix A** and set out as below:

- Users shall 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 shall 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 employee that has 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.
- If configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.
- NHS laptops shall never be (via cable or wireless) directly connected to other non-NHS IT equipment or systems.
- Users shall not use privately owned storage devices or storage devices owned by third parties for transfers of NHS data.
- Any device lost or stolen shall be reported immediately to the organisations line manager, NHIS Service Desk and Information Governance team (or equivalent).

6.7. **Internet Acceptable Use Guidance**

Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. You should not base any business-critical decisions on information from the Internet that has not been independently verified.

- Internet access via the NHS infrastructure is provided for business purposes. For the purpose of 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.
- Users shall not download copyrighted material such as software, text, images, music and video 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.

7. Communication, Monitoring and Review

7.1. Managers are required to make staff aware of information governance related policies to include this Acceptable Use of the Network Policy during their induction period. This policy is included in the ICB suite of policies available on-line.

7.2. The Information Governance Steering Group is responsible for monitoring compliance and the effectiveness of this policy though the reporting of incidents and use of staff surveys.

7.3. Any individual who has queries regarding the content of this policy, or has difficulty understanding how this policy relates to their role, should contact the Information Governance Team.

8. Staff Training

8.1. Nottingham and Nottinghamshire ICB is required to ensure organisational compliance with legislation and Department of Health and Social Care guidelines relating to data security and data protection. This requires knowledge and awareness of data security and data protection to be at the core of the ICB's objectives and embedded amongst other governance initiatives.

8.2. Annual Data Security Awareness (DSA) Level 1 training, as developed by NHS Digital, is mandatory for all staff members, including new starters, locums, temporary staff, lay members, student and contract staff at Induction and on an annual basis as refresher training for staff..

8.3. This training is mandated for corporate induction and thereafter annually with a minimum target of 95% completion across the ICB. At Induction managers must provide staff with an Information Governance Staff Handbook that provides awareness of information security concepts and principles to ensure compliance with this policy but should more training be required please contact the Information Governance Team.

9. Equality and Diversity Statement

9.1. Nottingham and Nottinghamshire ICB pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation as a commissioner and provider of services, as well as an employer.

9.2. The ICB is committed to ensuring that the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary), marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.

9.3. We are committed to ensuring that our activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, roma and travellers.

9.4. As an employer, we are committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

9.5. To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to, this policy.

10. Interaction with other Policies

10.1. This policy document should be read in conjunction with:

- Confidentiality and Data Protection Policy
- Information Security Policy
- Internet and Email Policy
- Account Management and Access Policy
- Removable Media Policy
- Risk Management Policy
- Incident Reporting and Management Policy
- Information Governance Staff Handbook

11. References

11.1. This policy takes into account reviews of the following as part of the development of this policy document:

- Access to Health Records Act 1990
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulation 2016
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Equality Act 2010
- Fraud Act 2006
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Human Rights Act 1998
- ISO/IEC 27001:2005 & ISO/IEC27002:2005 Specification & Code for an Information Security Management system
- NHS Act 2006
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Public Records Act 1958
- Regulations under Health and Safety at Work Act 1974
- 2004 Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992

12. Equality Impact Assessment for this Policy

Date of assessment:	June 2022			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age[1]	None	Not Applicable	Not Applicable	Not Applicable
Disability[2]	Visual accessibility of this policy	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	Not Applicable
Gender identity (trans, non-binary)[3]	None	Not Applicable	Not Applicable	Not Applicable
Marriage or civil partnership status[4]	None	Not Applicable	Not Applicable	Not Applicable
Pregnancy or maternity[5]	None	Not Applicable	Not Applicable	Not Applicable

[1] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

[2] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

[3] The process of transitioning from one gender to another.

[4] Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[5] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

Date of assessment:	June 2022			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Race[6]	None	Not Applicable	Not Applicable	Not Applicable
Religion or belief[7]	None	Not Applicable	Not Applicable	Not Applicable
Gender[8]	None	Not Applicable	Not Applicable	Not Applicable
Sexual orientation[9]	None	Not Applicable	Not Applicable	Not Applicable
Carers[10]	None	Not Applicable	Not Applicable	Not Applicable

[6] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

[7] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

[8] A man or a woman.

[9] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[10] Individuals within the ICB which may have carer responsibilities.

APPENDIX A:

Acceptable Use of the Network 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

- You should avoid eating or drinking in the vicinity of any IT equipment. Spilling drinks or food on to keyboards, monitors or other IT equipment could cause serious damage. You should avoid exposing IT equipment to anything that may damage or prevent normal operation, such as: sudden impacts, excessive change in temperatures or humidity.
- Only authorised IT support personnel are allowed to open or move IT equipment or reconfigure or change system settings. You could cause serious damage if you attempt this yourself.
- When left unattended, even for a short period, you should ensure that you lock your terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete or windows + L function or other applicable method.
- You must ensure that you never leave portable equipment unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure. Although it should be avoided, if you have to leave portable equipment in parked cars, you must ensure it is completely invisible from outside the vehicle and protected from extreme temperatures. When traveling by air, you must ensure that Portable equipment is carried as hand or cabin luggage at all times and not checked in to the hold.
- If you are issued a Laptop or mobile devices it should only be used by you and not shared with or used by anyone else, including your work colleagues.

- Do not connect privately owned or non-NHS devices or use such devices with your NHS IT equipment or install unapproved or privately owned software on NHS IT equipment.
- You must ensure that any device lost or stolen is reported immediately to your local Security Team.

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 in order to limit storage requirements for non-business information.

You should 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.

Misuse of Information Systems

The use of NHS information or systems for malicious purposes or other than they were intended for could be deemed a disciplinary offence. This includes but is not limited to:

- Attempts to access external or internal systems you are not authorised for.
- Making discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or accessing such material; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.

- Acquiring or sending pornographic or material identified as offensive or criminal.
- Violating copyright or intellectual property rights, including use of obviously copyright-violated software.
- Accessing or attempting to access medical or confidential information without a legitimate purpose and prior authorisation.