Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

REMOTE WORKING POLICY

POLICY

Reference	ISP 09		
Approving Body	Information Governance Committee		
Date Approved	14th April 2023		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	x		
Issue Date	April 2023		
Version	7		
Summary of Changes from Previous Version	The policy has been revised in line with current NHS Digital Guidance. Appendix 1 updated February 2018.		
Supersedes	6		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Committee		
Date of Completion of Equality Impact Assessment	10th February 2023		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Potential non-compliance with: • Data Protection Legislation • The Computer Misuse Act 1990		
Target Audience	All Staff		
Review Date	April 2025		
Sponsor (Position)	Director of Corporate Affairs as Senior Information Risk Owner		
Author (Position & Name)	Information Governance Manager and Data Protection Officer		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Governance Team Nottinghamshire Health Informatics Service		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
Not Applicable	Not Applicable
Template control	June 2020

CONTENTS

APPENDICIES

1.0 INTRODUCTION

This policy has been developed to ensure that those with a business requirement to access Sherwood Forest Hospitals NHS Foundation Trust (the Trust) systems remotely or to use mobile devices in a standalone mode do so securely, and without introducing unacceptable threats to both the processing of information and the networked system.

Remote access is a method of accessing files and systems that can only usually be accessed from an NHS site or by using an authorised Virtual Private Network (VPN) token.

Due to changing working practices and the development of technology, remote access to systems by NHS staff (including Medirest, Skanska, agency and contractor colleagues) is now seen as an important way of working. Remote access can only be undertaken using approved and authorised devices.

Often, critical business processes rely on easy and reliable access to organisational information systems. This document sets out the policy for, holding, obtaining, recording, using and sharing information by remote access via the use of mobile devices and includes a set of common controls, which can be applied to reduce the risks associated with a remote access function.

2.0 POLICY STATEMENT

This policy:

- Identifies processes to ensure remote access is agreed and managed in line with the Information Security Policy and with the organisational business requirements.

- Ensures that access to information away from the organisation is conducted in a secure and confidential environment.

- Ensures the appropriate use of mobile devices, which includes portable computers such as laptops, notebooks, tablets, mobile telephones and smart phones

- Outlines the principles of accessing, processing and transferring information using home computers and mobile devices, in dispersed locations.

This policy covers all staff working for or on behalf of the organisation and includes:

- Travelling users (e.g. staff working across sites or are temporarily based at other locations).

- Home workers (e.g. IT support, Corporate Managers, IT Development staff, Clinicians).

- Non NHS staff (e.g. Social Services, contractors and other 3rd party organisations when authorised to access NHS systems).

The purpose of this policy is:

- To provide effective controls to ensure secure and resilient remote access to information systems.

- Ensure the confidentiality, integrity and availability of information accessed via a remote access solution.

- To ensure that information security is maintained when users access data on standalone mobile devices.

- To ensure the processing of information is operated in accordance with national guidance such as Department of Health Codes of Practice, ISO 27001: 2017 – Information Security Management , Data Protection Legislation, Caldicott Principles and local organisational and NHS policies.

- To ensure that all staff are aware of their responsibilities and comply with the policy and that the areas covered in this policy are part of information governance and IT training.

- This policy forms part of an overall group of Information Governance Policies, and should be read in conjunction with these.

- An equality Impact Assessment (EIA) has been carried out and has concluded that this policy is of low impact.

- Failure by any employee of the Trust to adhere to the policy and its guidelines will be viewed as a serious matter and may result in disciplinary action.

3.0 DEFINITIONS/ ABBREVIATIONS

User - In this policy, the term ‘user’ includes anyone who makes use of the Trust’s network or computing facilities to gain access to systems and applies specifically to: -

- All staff (including Medirest, Skanska, agency and contractor colleagues).

- Any authorised individual using Trust systems as a trainee, student, contractor, volunteer or otherwise.

The Trust – Sherwood Forest Hospitals NHS Foundation Trust (SFHFT)

Mobile Devices – This includes but is not limited to portable computers such as laptops, notebooks, tablets, mobile telephones, and smart phones.

Remote working - a work arrangement that permits an employee to conduct all or some of their work at an approved alternative worksite such as the home
Token - An electronic 1-time password generation device, which is used to enable remote access to information systems and applications. This token works through dedicated software being installed on a device.

NHIS - Information Communication and Technology services are provided by Nottinghamshire Health Informatics Service, who is hosted by Sherwood Forest Hospitals NHS Foundation Trust.

4.0 ROLES AND RESPONSIBILITIES

Committees

Trust Board
The Trust Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Information Governance Committee
The Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

Chief Executive
The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner
The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated SIRO, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer

We are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Information Asset Owners (IAOs)

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)

Information Asset Administrators ensure that IG policies and procedures are followed, recognise actual or potential IG security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Directors and Services Managers

Responsible for ensuring a comprehensive risk assessment is undertaken regarding the safety and security of the health records during transport to and from, and while present at non Trust premises. Completed risk assessments should be submitted to the Information Asset Owner for evaluation and approval by the Medical Records Advisory Group, also ensure that risk assessments are accurately maintained and risks re-evaluated and updated if significant changes are made to services.

Duty Nurse Managers

Out-of-hours or on occasions when the Caldicott Guardian, Information Governance Manager or Information Asset Owner are unavailable, Duty Nurse Managers in the first instance will be required to assume responsibility for any decision regarding urgent disclosures that cannot be delayed, they can if necessary seek assistance from staff involved in the Gold/Silver On-Call Protocol consulting with the Trust's Legal Advisors as necessary.

All Staff

All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of IG security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors. Any IG security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our policy and accept their personal responsibility to maintain confidentiality at all times.

All staff will 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. All staff are responsible for ensuring that no actual or potential security breaches occur as a direct result of their actions.

All staff with remote access and/or use mobile devices are responsible for complying with this policy and associated standards. All staff must safeguard organisational equipment and information resources, and notify the Trust immediately of any security incidents and breaches. Users must return all relevant equipment (including software) to their line manager when remote access and/or the mobile device are no longer required.

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

The Service Desk (NHIS) will action requests for remote access on receipt of an appropriately authorised request as per the form at Appendix 2.

5.0 APPROVAL

Policy approval is by the Information Governance Committee.

6.0 DOCUMENT REQUIREMENTS

With regard to the equipment, the remote worker will be expected to:

• Take reasonable care of the equipment;

• Take all reasonable steps to minimize the risk of theft or damage to Trust property and paperwork whilst these items are away from Trust premises;

• Use it only for work purposes and in accordance with any operating instructions as defined in the Information Security Policy;

• Comply with software licensing Terms and Conditions;

• Return to the Trust, the equipment at the end of the Remote working arrangement

Remote Access Process

Remote access refers to any technology that enables a user to connect in geographically dispersed locations to Trust owned systems. Remote access is typically over a broadband network, although it can include Wide Area Network (WAN) connections.

It is the responsibility of the relevant line manager to submit a request for remote access on behalf of their staff. Applications for remote access should be submitted via email or using the customer portal http://customerportal.notts-his.nhs.uk/ to the Nottinghamshire Health Informatics Service (NHIS) Service Desk for action using the Application for Remote Access form (Appendix 2).

Each application must include reasonable justification for users to have remote access to administrative and/or clinical systems, outlining the high-level requirement for each request.

With each application, the Head of Department or Service must be aware that to support remote access, provision of equipment including in some cases line installations, must be provided from departmental budgets. Furthermore, all recurrent costs of line rental, maintenance etc. must be met by departmental budget.

Accessing Information Remotely

The direct connection of mobile devices to the organisation's network requires prior authorisation. This is in line with the Trust's Information Security Policy and further information regarding this can be obtained from the Information Governance Team.

All mobile devices are protected with the appropriate level of encryption in line with the guidance and good practice developed by NHS England. Devices must be password and/or PIN number protected, depending on the mobile device. Only authorised and approved devices are permitted to connect to the Trust's network.

Mobile Device Security

Mobile devices must never be left unattended in cars or easily accessible areas to reduce the risk of opportunistic theft. If possible devices should be kept securely locked away when not in use.

Care should also be taken during transit. Heavy jolts to a mobile device could cause damage to the hard disk and render the system inoperable.

Virus protection software must be installed, active and up to date. Laptops must be connected to the network on a regular basis (at least monthly) for 1-2 hours to ensure that anti-virus, applications and operating system updates are applied to the device.

Staff should also refer to the Trust's Information Security Policy.

Storage Device Security

Personal confidential data must not be stored on any mobile media storage devices (e.g. CDs USB devices etc.), unless the information and/or device is encrypted to the recognised NHS standard.

Note: NHIS WILL NOT support equipment purchased outside of the NHS or not in the NHIS Service Catalogue.

Appropriate Use of Mobile Devices

To ensure information on a mobile device is backed up, this should be transferred to network storage on a regular basis. This is to ensure the live record remains up to date and minimises the risk of information being lost.

Unauthorised software must not be installed on any organisational equipment, including mobile devices.

Confidential information must not be sent via email unless this complies with the Email and Internet Policy.

All mobile devices must be returned to line managers for re-use or secure destruction when a staff member leaves.

Data from mobile devices must be securely erased as per the NHIS Disposal of IT Equipment and Media Policy

Equipment is approved and issued for the sole use of that individual. Devices must not be passed on to other staff without prior permission of the appropriate Service Line Manager

The Trust reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. On behalf of the Trust NHIS will engage in such action if such equipment is being used in a way that puts the company's systems, data, users, customers or partners personal confidential data at risk

Users must ensure that Virus protection software or any other security measures put in place on devices are never disabled or bypassed

Monitoring Compliance

To ensure the most comprehensive level of protection possible, the network includes security components that address the following five aspects of network security.

1. User Identity

All remote users must be registered and authorised. User identity will be confirmed by User ID and password authentication. A log of remote users is maintained in the application software by the NHIS Service Desk. It is the line manager's responsibility to ensure that the Service Desk is notified of any leavers, and staff no longer needing remote access (e.g. change of role/department), in order to remove access to clinical applications.

2. Perimeter Security

NHIS is responsible for ensuring perimeter security devices are in place and operating properly. Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. Routers and switches handle this access control with access control lists and by dedicated firewall appliances.

Remote Access Systems with strong authentication software control remote dial in users to the network. A firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorised traffic to pass, according to a predefined security policy. Complementary tools, including virus scanners and content filters, also help control network perimeters.

3. Security Monitoring

Network vulnerability scanners are used to identify areas of weakness, and intrusion detection systems to monitor and reactively respond to security events as they occur.

4. Remote diagnostic services and 3rd parties

External suppliers and third parties that require access to their systems through the network to investigate/fix faults are allowed through remote Health and Social Care Network (HSCN) connection and secure 1-time password token.

Each supplier or user requiring remote access is required to commit to maintaining confidentiality of data and information and only using qualified representatives.

Each request for dial up access will be authorised by the approved NHIS engineers, who will only make the connection when satisfied that security precautions are in place.

5. Encryption Software

All mobile devices must have appropriate encryption software installed.

Access to the organisation's Infrastructure

Remote access to the organisation's infrastructure is via secure token.

Tokens are issued through the NHIS. Issue will be subject to completion of the 'Application for Remote Access' form in Appendix 2, which includes a description of why the access is required, and has been endorsed by the Line Manager.

All users of tokens must comply with the Information Security Policy, Policy on the Acceptable Use of the Internet and Electronic Mail and the Confidentiality Policy.

It is the responsibility of the person who holds the token to ensure that this is ALWAYS held in a safe and secure manner. The following principles are in addition to the responsibilities outlined by the above-named policies, and must ALWAYS be observed.

- NO other person (including family members) should be able to overlook what data is being accessed by the user.

- If a machine is left for even a short time, then it MUST be screensaver locked or the user can press Ctrl+Alt+Delete and then Enter (or Windows Key + L) to lock the screen.

- Any VPN connection must be correctly terminated once all remote work has been completed to ensure that the applications are closed appropriately.

- If the token is lost / stolen / misplaced, this MUST be reported to the NHIS Service Desk as an incident IMMEDIATELY.

- Devices must be connected to the NHS network on a regular basis to ensure that applications and operating systems remain up to date.

Remote Access and Smartcard Access

Gaining access to certain programmes via Remote Access (e.g. from home) may also require Smartcard sign in.

Users wishing to gain access to these systems will need to install a Smartcard reader and software onto the remote computer. Remote access to these systems should be instigated by the Head of Department or Service. The NHIS Service Desk will provide advice on installing the Smartcard reader and software.

Smartcard policies and procedures must be followed.

Reporting Security Incidents and Weaknesses

All security incidents and weaknesses must be reported using the Trust's Incident Reporting mechanisms and Datix system and the NHIS Service Desk notified.

7.0 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 (eg verbal, formal report etc) and by who)**
DSPT Validation	360 Assurance	Audit	Annually	IG Committee
Adherence to Information Security policy and guidelines in nominated Division/Corporate Function	IG Committee	Audit	Annually	IG Committee
IAO report to the SIRO for each division including reference to security incidents and risks (Copy available from IG office)	IAO	Self-Assessment Return	Annually	IG Manager/ SIRO
Network security monitoring and reporting by NHIS	NHIS	Report shared	TBC	IG Committee

8.0 TRAINING AND IMPLEMENTATION

8.1 Training

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.

8.2 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]

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document is not subject to an Environmental Impact Assessment.

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

The legal obligations of the Trust and the NHS can be found in the NHS Information Governance Guidance on Legal and Professional Obligations (DH, 2007) which is available on the Intranet and this policy must be read in the context of and regarding these legislations and guidance.

This policy should be read in conjunction with the Information Security Policy, Internet and Email Policy and Confidentiality Policies which are available on the Trust's website.

Evidence Base:

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

- Data Protection Act 2018 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- UK General Data Protection Regulation Guide to the UK General Data Protection Regulation (UK GDPR) | ICO
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Human Rights Act 1998.

National Guidance

- ISO/IEC 27001:2017
- Information Security Management: NHS Code of Practice 2007
- NHS Code of Confidentiality 2016

Related SFHFT Documents:

- Confidentiality Audit Policy
- Data Protection, Confidentiality and Disclosure Policy Data Protection, Confidentiality and Disclosure Policy
- Email and Internet Policy
- Information Governance Policy
- Information Security Policy
- Data Protection Impact Assessment Policy
- Safe Haven Procedure

11.0 KEYWORDS

words ***not*** in the published title but thought useful when using the intranet search engine to help find the document

12.0 APPENDICES

- Appendix 1 - Equality Impact Assessment
- Appendix 2 - Application for Remote Access
- Appendix 3 - Mobile Devices - Guidance Note

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Electronic Remote Working Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 10th February 2023			
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	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

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

- Trust guidance for completion of the Equality Impact Assessments

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: Gina Robinson, Information Security Officer

Signature:

Date: 10th February 2023

APPENDIX 2 - APPLICATION FOR REMOTE ACCESS

Please complete the following fields in order to obtain remote access to the Nottinghamshire Health Informatics Service' network. Once complete please send the form to the NHIS via email nhis.servicedesk@notts-his.nhs.uk

***** Note: Remote Access will only be provided for use on NHS supported devices *****

	User Details	Line Manager Details
Full Name		
Organisation Name		
Base		
Job Title		
Windows Username		
Contact Tel No.		
Email Address		

TYPE OF ACCESS REQUIRED:

	Required	Make of smartphone
Vasco Soft Token (access via your smartphone or tablet)		
Hard Token - Reassignment only	Previous User: Token ID:	

I can confirm that I have read and understood the organisations Electronic Remote Working Policy and am up to date with mandatory Information Governance Training.
I understand my responsibilities about information confidentiality and security whilst working remotely.

User Signature ……..*
Date……..

Line Manager Signature…… *
Date……..

* Please note we cannot accept typed signatures

APPENDIX 3 - MOBILE DEVICES - GUIDANCE NOTE

Laptops and other mobile devices taken outside secure NHS environments are subject to special security risks. Mobile devices include such items as laptops, smart phones, iPads, memory sticks, notebooks and any other mobile email device capable of storing data.

We all have an obligation as NHS employees to ensure the safe and secure processing of NHS data both in and out of NHS premises. The following guidelines will help you take the necessary precautions against loss and theft and will also reduce the risk of information being disclosed to unauthorised individuals.

- Guidance from the UK Government states specifically that **no** personal confidential data be held on any mobile devices unless it is encrypted to the approved standard, 256bit
- DO NOT leave mobile devices unattended
- Ensure laptops are stored securely out of sight and do not leave laptops unattended in car boots overnight
- Carry your laptop in a protective anonymous bag
- Make sure you take regular backups of the work you complete on your laptop and store these securely
- Use passwords on all systems to minimise potential data exposure
- Do not allow anyone else to use your devices under your logon
- Ensure your password and token (if used) is **not** stored or kept with the laptop
- Change passwords regularly and when prompted in line with NHIS corporate policy and save information to a shared drive as soon as possible.
- Perform regular housekeeping tasks such as deleting old and unneeded files.
- Only authorised and licensed software and files may be installed on any mobile device.
- Only devices authorised by NHIS can be connected to the network.
- Employees should never disclose their passwords or PIN details.
- In the event of a lost or stolen device, the user should report as an incident as soon as possible
- Individuals must not make any modifications to the hardware or software installed on the device.