Outstanding Care,
Compassionate People,
Healthier Communities

Sherwood Forest Hospitals
NHS Foundation Trust

# REMOTE WORKING POLICY

**POLICY**

| | | |
|---|---|---|
| **Reference** | ISP 09 | |
| **Approving Body** | Data Protection and Cyber Security Committee | |
| **Date Approved** | 17th November 2025 | |
| **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** |
| | x | |
| **Issue Date** | January 2026 | |
| **Version** | 8 | |
| **Summary of Changes from Previous Version** | Information that is available in the Trust's Information Security Policy has been removed to avoid duplication | |
| **Supersedes** | 7 | |
| **Document Category** | • Information Governance | |
| **Consultation Undertaken** | Data Protection and Cyber Security Committee<br>Cyber Security Assurance Programme Board | |
| **Date of Completion of Equality Impact Assessment** | 11th November 2025 | |
| **Date of Environmental Impact Assessment (if applicable)** | Not applicable | |
| **Legal and/or Accreditation Implications** | Potential non-compliance with:<br>• Data Protection Legislation<br>• The Computer Misuse Act 1990 | |
| **Target Audience** | All Staff | |
| **Review Date** | November 2027 | |
| **Sponsor (Position)** | Senior Information Risk Owner | |
| **Author (Position & Name)** | Head of Data Security and Privacy 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<br>Nottinghamshire Health Informatics Service | |

| **Associated Documents/ Information** | **Date Associated Documents/ Information was reviewed** |
|---|---|
| Not Applicable | Not Applicable |

## Contents

## 1.0 INTRODUCTION

Being responsible for compliance with the UK GDPR and Data Protection Act means that we need to be proactive and organised about our approach to data protection. The Data (Use and Access) Act 2025 introduces new lawful bases for processing, enhanced transparency obligations, and expanded ICO powers. All data transfers must comply with the Data (Use and Access) Act provisions alongside UK GDPR and Data Protection Act 2018. The Data (Use and Access) Act introduces a new lawful basis ("recognised legitimate interest") for certain public interest activities that will be implemented and enforceable from June 2026. The policy will be updated as ICO guidance evolves.

Under Article 24(1) of the UK GDPR, organisations are obligated to implement technical[1] and organisational measures that both ensure and demonstrate compliance with the UK GDPR. These measures should be risk-based and proportionate to the nature of the data processing activities being undertaken. Furthermore, such measures must be reviewed and updated as necessary to maintain ongoing compliance.

This policy has been established to ensure that individuals with a legitimate business requirement to access systems of the Sherwood Forest Hospitals NHS Foundation Trust (the Trust) remotely, or to utilise mobile devices in a standalone capacity, do so in a manner that is secure and does not present unacceptable risks to information processing or to the networked environment.

Remote access is defined as a means of connecting to files and systems that are otherwise only accessible directly from an NHS site or through the use of an authorised Virtual Private Network (VPN) token.

As working practices evolve and technology advances, remote access for NHS staff—including Medirest, Skanska, agency, and contractor colleagues—has become an essential component of modern working. It is important to note that remote access must be performed exclusively using devices that have been duly approved and authorised.

Critical business processes are often dependent on straightforward and reliable access to organisational information systems. This policy document details the procedures for holding, obtaining, recording, using, and sharing information through remote access with mobile devices. It incorporates a set of standardised controls designed to mitigate the risks associated with providing remote access functionality.

## 2.0 POLICY STATEMENT

This policy:

- Specifies procedures to ensure that remote access is authorised and managed in accordance with the Information Security Policy and the organisation's business requirements.

- Ensures that information accessed outside the organisation is handled within a secure and confidential setting.
- Mandates the appropriate use of mobile devices, including but not limited to portable computers such as laptops, notebooks, tablets, mobile telephones, and smart phones.
- Outlines the core principles for accessing, processing, and transferring information using home computers and mobile devices, regardless of location.

The scope of this policy extends to all staff working for or on behalf of the organisation, including:

- Travelling users, such as staff who work across multiple sites or who are temporarily based at other premises.
- Home workers, including IT support, Corporate Managers, IT Development staff, and Clinicians.
- Non-NHS staff, for example, Social Services, contractors, and other third-party organisations, when they are authorised to access NHS systems.

The aims of this policy are:

- To establish effective controls ensuring secure and resilient remote access to information systems.
- To maintain the confidentiality, integrity, and availability of information accessed through remote access solutions.
- To safeguard information security when users access data via standalone mobile devices.
- To ensure that all information processing complies with national guidelines, including Department of Health Codes of Practice, ISO 27001:2017 (Information Security Management), Data Protection Legislation, Caldicott Principles, and both local organisational and NHS policies.
- To ensure that all staff are informed of their responsibilities, comply with this policy, and that the topics addressed are incorporated into information governance and IT training.

This policy forms part of the broader suite of Information Governance Policies and should be read in conjunction with them.

Failure by any Trust employee to comply with this policy and its associated guidelines will be considered a serious offence and may lead to disciplinary action.

## 3.0 DEFINITIONS/ ABBREVIATIONS

This section outlines the key terms and abbreviations used throughout this policy to ensure clarity and consistency of understanding among all users.

- **Mobile Devices** - as referenced in this policy, encompass a range of portable computing equipment. This includes, but is not limited to, laptops, notebooks, tablets, mobile telephones, and smart phones.
- **NHIS** stands for Nottinghamshire Health Informatics Service. This service is responsible for providing Information Communication and Technology (ICT) services and is hosted by Sherwood Forest Hospitals NHS Foundation Trust.
- **Remote Working** - describes an arrangement whereby an employee is permitted to undertake all or part of their work from an approved alternative worksite, such as their home. This term applies specifically to working offsite from a non-fixed location using mobile devices such as laptops, tablets, or smartphones.
- **The Trust** - Throughout this document, 'the Trust' refers to Sherwood Forest Hospitals NHS Foundation Trust (SFHFT).
- **Token** - A token refers to an electronic device that generates a one-time password, which is required to enable secure remote access to information systems and applications. The token's functionality is dependent upon the installation of dedicated software on the user's device.
- **User** - For the purposes of this policy, a 'user' is defined as any individual who utilises the Trust's network or computing facilities to access information systems. This specifically includes all employees, such as those directly employed by the Trust as well as staff from partner organisations like Medirest and Skanska, agency staff, and contractor colleagues. Additionally, it covers any authorised individuals who may use Trust systems in a capacity such as trainee, student, contractor, or volunteer.

## 4.0 ROLES AND RESPONSIBILITIES

### Trust Board

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

### Data Protection and Cyber Security 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 Data Protection and Cyber Security Committee.

### Senior Information Risk Owner

The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner , 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 Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

**Caldicott Guardian**

The Caldicott Guardian role is carried out by the Chief Medical Officer (CMO). The Caldicott Guardian 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) are 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 Information Governance policies and procedures are followed, recognise actual or potential Information Governance 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.

**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. 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 other information security policies.

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 Information Governance security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors. Any Information Governance security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team.

All actual or suspected data breaches must be reported immediately in line with the Trust's incident reporting policy. The Data Protection Officer will determine if it's necessary to notify the ICO or report to the Data Security Protection Toolkit and will take action within 72 hours if required.

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.

## 5.0 APPROVAL

This policy is approved by the Data Protection and Cyber Security Committee.

## 6.0 DOCUMENT REQUIREMENTS

### 6.1 Remote Access Process

Remote access to the Trust's network is strictly controlled and requires prior authorisation in accordance with the Trust's Information Security Policy. Staff seeking further information or clarification should contact the Information Governance Team.

Requests for remote access must be submitted by the relevant line manager on behalf of their staff members. All applications should be made through the NHIS customer portal.

It is also the responsibility of the relevant line manager to promptly notify the NHIS Service Desk regarding staff who are leaving, or those whose roles or departments have changed and who no longer require remote access. This ensures that access to clinical applications is revoked in a timely manner, maintaining the security of the Trust's systems.

Soft tokens required for remote access are issued through NHIS.

### 6.2 Mobile Device Security

- Mobile devices must never be left unattended in vehicles or areas where they could be easily accessed, as this increases the risk of opportunistic theft. When not in use, mobile devices should be kept secure and locked away to prevent unauthorised access.
- Particular care should be taken when mobile devices are being transported. Heavy jolts or impacts can cause significant damage to the hard disk, potentially rendering the device unusable.
- Staff are advised to consult the Trust's **Information Security Policy, specifically Appendix 3**, for further guidance on the secure use and handling of mobile devices.
- Mobile devices must not be transferred or passed on to other members of staff without the prior permission of the appropriate line manager.
- All remote users must be registered and authorised. User identity will be confirmed through User ID and password authentication. NHIS maintains a log of remote users.

### 6.3 Storage Device Security

NHIS will only provide support for equipment that has been procured through the NHS and is included in the NHIS Service Catalogue. Equipment purchased externally or not listed in the catalogue will not be supported by NHIS.

### 6.4 Incident Reporting

All data security and cyber security incidents must be reported on Datix, in line with the Trust's Incident Reporting Policy and the NHIS Service Desk notified.

If the hard token is lost or stolen, this MUST be reported as soon as possible to the NHIS Service Desk.

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

## 7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

| Minimum Requirement to be Monitored<br>(WHAT – element of compliance or effectiveness within the document will be monitored) | Responsible Individual<br>(WHO – is going to monitor this element) | Process for Monitoring e.g. Audit<br>(HOW – will this element be monitored (method used)) | Frequency of Monitoring<br>(WHEN – will this element be monitored (frequency/ how often)) | Responsible Individual or Committee/ Group for Review of Results<br>(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g verbal, formal report etc) and by who) |
|---|---|---|---|---|
| Data Security Protection Toolkit validation | 360 Assurance | Audit | Annually | Data Protection and Cyber Security Committee |
| Adherence to information security policy and guidelines in nominated division/corporate function | Data Protection and Cyber Security Committee | Audit | Annually | Data Protection and Cyber Security Committee |
| IAO report to the SIRO for each division including reference to security incidents and risks (Copy available from Information Governance office) | IAO | Self-Assessment Return | Annually | Head of Data Security and Privacy/ SIRO |
| Network security monitoring and reporting by NHIS | NHIS | Report shared | TBC | Data Protection and Cyber Security 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:**

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

[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/

- UK General Data Protection Regulation Guide to the UK General Data Protection Regulation (UK GDPR) | ICO
- Data (Use and Access) Act 2025
- 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
- NCSC Advice and Guidance: https://www.ncsc.gov.uk/section/advice-guidance/you-your-family

**Related SFHFT Documents:**

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

## 11.0 KEYWORDS

VPN.

## 12.0 APPENDICES

- Refer to list in contents table

## APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

### EIA Form Stage One:

| | | |
|---|---|---|
| **Name EIA Assessor: Gina Robinson** | | **Date of EIA completion: 11th November 2025** |
| **Department: Information Governance** | | **Division: Corporate** |
| **Name of service/policy/procedure being reviewed or created: Remote Working Policy** | | |
| **Name of person responsible for service/policy/procedure: Director of Corporate Affairs** | | |
| **Brief summary of policy, procedure or service being assessed: process and guidance for remote workers** | | |
| **Please state who this policy will affect: Staff** | | |
| **Protected Characteristic** | **Considering data and supporting information, could protected characteristic groups' face negative impact, barriers, or discrimination? For example, are there any known health inequality or access issues to consider? (Yes or No)** | **Please describe what is contained within the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening.<br>Please also provide a brief summary of what data or supporting information was considered to measure/decipher any impact.** |
| **Race and Ethnicity** | No | Not applicable. |
| **Sex** | No | |
| **Age** | No | |
| **Religion and Belief** | No | |
| **Disability** | No | |
| **Sexuality** | No | |
| **Pregnancy and Maternity** | No | |
| **Gender Reassignment** | No | |
| **Marriage and Civil Partnership** | No | Not applicable. |

| | | |
|---|---|---|
| **Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)** | No | |

**If you have answered 'yes' to any of the above, please complete Stage 2 of the EIA.**

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

**None.**

**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.**

**On the basis of the information/evidence/consideration so far, do you believe that the policy / practice / service / other will have a positive or negative adverse impact on equality?** (delete as appropriate)

| Positive | | | Negative | | | |
|---|---|---|---|---|---|---|
| **High** | **Medium** | **Low** | **Nil** | **Low** | **Medium** | **High** |

**If you identified positive impact, please outline the details here:**

The policy is written 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.

## EIA Form Stage Two:

| Protected Characteristic | Please explain, using examples of evidence and data, what the impact of the Policy, Procedure or Service/Clinical Guideline will be on the protected characteristic group. | Please outline any further actions to be taken to address and mitigate or remove any in barriers that have been identified. |
|---|---|---|
| **Race and Ethnicity** | | |
| **Gender** | | |
| **Age** | | |
| **Religion** | | |
| **Disability** | | |
| **Sexuality** | | |
| **Pregnancy and Maternity** | | |
| **Gender Reassignment** | | |
| **Marriage and Civil Partnership** | | |
| **Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)** | | |

| |
|---|
| **Signature:**<br><br>*I can confirm I have read the Trust's Guidance document on Equality Impact Assessments prior to completing this form* |
| **Date:** |
| **Please send the complete EIA form to the People EDI Team for review.**<br>**Please send the form to: sfh-tr.edisupport@nhs.net** |