Ashford and St. Peter's Hospitals
NHS Foundation Trust

Remote Access Policy

Author: **Head of IT**

Executive Lead: **Simon Marshall, Director of Finance and Information**

Status: Approval date: Jan 2019

Ratified by: Information Governance Steering Group

Review date: Jan 2022

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Author
1	Sept 2010	Amendments to Job Titles and Departmental names to reflect organisational changes. Addition of Monitoring and Review of Policy.	Head of IT
2	Dec 2012	Amendments to names and titles Amendments to cover non-Trust-owned PC's	Head of IT
3	Dec 2015	Amendment to authorisation manager	Head of IT
4	Dec 2018	Updated Executive summary, sections 1 – 8	Head of IT
5	Jan 2019	Updated sections 13 and 14	Head of IT

For more information on the status of this document, please contact:	
Policy Author	Malcolm Flier - Head of IT
Department/Directorate	Health Informatics / Finance
Date of issue	Jan 2019
Review due	Jan 2022
Ratified by	Information Governance Steering Group
Audience	All Staff

Executive summary

Remote Access by staff and other non-NHS organisations is a method of accessing files and systems from remote locations away from the Trust's main campuses. Critical business processes rely on easy and reliable access to corporate information systems so that business can be conducted remotely with confidence and sensitive corporate information can remain confidential. This document sets out the policy for remote access in order to reduce the risks associated with the service.

Contents

SECTION **Page**

Appendices

See also: Any relevant trust policies/guidelines or procedures

1. Introduction

1.1 Remote access by staff and other non-NHS organisations is a method of accessing files and systems. Critical business processes rely on easy and reliable access to corporate information systems so that business can be conducted remotely with confidence and sensitive corporate information can remain confidential.

2. Scope

2.1 This policy covers all types of remote access including:

- Travelling users (e.g. staff temporarily based at other locations)
- Home workers (e.g. IT staff, managers, clinicians)
- Non-NHS staff (e.g. contractors and third-party organisations)

3. Purpose

The objectives of the Trust's policy on remote access by staff are:

3.1 To provide secure and resilient remote access to the Trust's information systems.

3.2 To preserve the integrity, availability and confidentiality of the Trust's information and information systems.

3.3 To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.

3.4 To comply with all relevant regulatory and legislative requirements (including data protection laws and regulations) and to ensure that the Trust is adequately protected under computer misuse legislation.

4. Explanation of Terms Used

RAS – Remote Access Service.

5. **Duties and responsibilities**

5.1 The Trust Board is ultimately responsible for ensuring that remote access by staff is managed securely.

5.2 The Information Governance Steering Group will govern policy and standards, and the IT Department will manage and maintain procedures for remote access to ensure that risks are identified and appropriate controls implemented to reduce those risks.

5.3 The Head of IT is responsible for providing clear authorisation for all remote access users and the level of access provided.

5.4 The Head of IT is responsible for confirming whether remote access to business applications and systems is permitted.

5.5 The IT Department will ensure that user profiles and logical access controls are implemented in accordance with agreed access levels.

5.6 All remote access users are responsible for complying with this policy and associated Trust policies and standards. They must safeguard corporate equipment and information resources and notify the Trust immediately of any security incidents and breaches using the Datix reporting system.

5.7 Users must return all relevant equipment on termination of the connections.

5.8 The Head of IT is responsible for assessing risks and ensuring that controls are being applied effectively.

6. Policy

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

User Identify

6.1 All remote users must be registered and authorised by the Head of IT User identity will be confirmed by strong two factor authentication (user ID and password plus a physical token). The IT Department is responsible for ensuring a log is kept of all user remote access.

Perimeter Security

6.2 The IT Department will be 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. Remote access systems with strong authentication software control remote users of 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.

Secure Connectivity

6.3 The Trust will protect confidential information from eavesdropping or tampering during transmission.

Remote Diagnostic Services and Third Parties

6.4 Suppliers of central systems/software expect to have remote access to such systems on request to investigate/fix faults. The Trust will permit such access subject to Trust procedures being adhered to and all activity being monitored.

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

6.6 The Trust recognises that by providing staff with remote access to information systems, risks are introduced that may result in serious business impact, for example:

- Unavailability of network, systems or target information
- Degraded performance of remote connections
- Loss or corruption of sensitive data
- Breach of confidentiality
- Loss of or damage to equipment
- Breach of legislation or non-compliance with regulatory or ethical standards

6.7 The security architecture is integrated into the existing Trust network and is dependent on the IT security services that are offered through the network infrastructure.

These are:

- Password authentication, authorisation and accounting
- Strong two-factor authentication

6.8 When a non-Trust owned device is used to connect to RAS, downloading of files to that non-Trust device will be blocked. Similarly, no email attachments will be allowed to be downloaded.

6.9 All security incidents and weaknesses must be reported following the Trust's Policy for the Reporting and Management of Incidents (typically Datix).

6.10 The IT Department based at Ashford and St Peter's will provide support for the Remote Access service.

- This support is limited to Trust-supplied hardware and Trust-hosted software. Support for Trust equipment will be provided only if the device is brought in to the Trust.
- Support for Home PCs, the software thereon, and any peripheral equipment such as printers or routers, is the responsibility of the owner or householder.
- Provision of, and support for the link between a PC/laptop at home and the internet, and any associated equipment, is the responsibility of the owner or householder.

7. Training

7.1 The Trust will ensure that all users of information systems, applications and the networks are provided with necessary security guidance, awareness and where appropriate training to discharge their security responsibilities. Irresponsible or improper actions may result in disciplinary action.

7.2 In order to access certain services, the user may be required to provide current, accurate identification, contact, and other information as part of the registration process and/or continued use of the Remote Access Service.

7.3 The user is responsible for maintaining the confidentiality of their account password and is responsible for all activities that occur under their account. The user must immediately notify the IT Department of any unauthorised use of their password or account or any other breach of security.

7.4 The Trust cannot and will not be liable for any loss or damage arising from the user's failure to provide the Trust with accurate information or to keep their password secure.

8. Stakeholder Engagement and Communication

8.1 The policy has been written by the Health Informatics Team and is reviewed and approved by the Information Governance Steering Group. The policy is available to all staff on TrustNet.

8.2 All new staff are referred to this policy at Induction. Staff are instructed to read this policy when they agree to the terms for remote access.

9. Approval and Ratification

9.1 Ratification of this policy will be sourced from the Information Governance Steering Group.

10. Dissemination and Implementation

10.1 The policy will be disseminated through the Aspire global email.

10.2 This policy will be published on the Trust intranet and internet sites.

11. Review and Revision Arrangements

11.1 This policy will be reviewed by the author every 3 years, or before if necessary.

12. Document Control and Archiving

12.1 This is a Trust-wide document and archiving arrangements are managed by the Head of Regulation & Accreditation and the Information Content Manager (Quality and Communications Teams) who can be contacted to request master/archived copies.

12.2 On the internet site, the document will be highlighted as green when in date, amber 3 months prior to review date, and red if expired.

13. Monitoring compliance with this Policy

This document will be monitored regularly to ensure it is effective and to assure compliance

Requirement to be monitored	Leads	Tool	Frequency of monitoring	Reporting Arrangements	Lead(s) for acting on recommendations
This policy will be regularly reviewed and updated	IT Department and Information Governance lead(s)	Report to Information Governance Steering Group	At least every 3 years or more frequently if required	HIS policy audit report to: Information Governance Steering Group	Assigned by Information Governance Steering Group

14. Supporting References / Evidence Base

14.1 Government guidance
14.2 Industry standards
14.3 NHS Digital generic guidance

APPENDIX 1: EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Summary

Name and title: Morné Beck – Head of IT
Policy: Remote Access Policy

Background

- Who was involved in the Equality Impact Assessment

The EIA was performed by the Head of IT

Methodology

- A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age)
- The data sources and any other information used
- The consultation that was carried out (who, why and how?)

The policies were examined and reviewed to ensure that no negative impact on equality would result from the policies.

Key Findings

- Describe the results of the assessment
- Identify if there is adverse or potentially adverse impacts for any equalities groups

There is no impact on equality.

Conclusion

- Provide a summary of the overall conclusions

The policies apply to all staff regardless of race, ethnic origin, gender, culture, religion or belief, sexual orientation and age.

Recommendations

- State recommended changes to the proposed policy as a result of the impact assessment
- Where it has not been possible to amend the policy, provide the detail of any actions that have been identified
- Describe the plans for reviewing the assessment

The policy should be approved.

APPENDIX 2: CHECKLIST FOR THE REVIEW AND APPROVAL OF DOCUMENTS

To be completed (electronically) and attached to any document which guides practice when submitted to the appropriate committee for approval or ratification.

Title of the document:
Policy (document) Author: Malcolm Flier, Head of IT
Executive Director: Simon Marshall, Director of Finance and Information

		Yes/No/ Unsure/ NA	Comments
1.	**Title**		
	Is the title clear and unambiguous?	**Yes**	
	Is it clear whether the document is a guideline, policy, protocol or standard?	**Yes**	
2.	**Scope/Purpose**		
	Is the target population clear and unambiguous?	**Yes**	
	Is the purpose of the document clear?	**Yes**	
	Are the intended outcomes described?	**Yes**	
	Are the statements clear and unambiguous?	**Yes**	
3.	**Development Process**		
	Is there evidence of engagement with stakeholders and users?	**Yes**	
	Who was engaged in a review of the document (list committees/ individuals)?		
	Has the policy template been followed (i.e. is the format correct)?	**Yes**	
4.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	**Yes**	
	Are local/organisational supporting documents referenced?	**Yes**	
5.	**Approval**		
	Does the document identify which committee/group will approve/ratify it?	**Yes**	
	If appropriate, have the joint human resources/staff side committee (or equivalent) approved the document?		
6.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	**Yes**	
	Does the plan include the necessary training/support to ensure compliance?		
7.	**Process for Monitoring Compliance**		

		Yes/No/ Unsure/ NA	Comments
	Are there measurable standards or KPIs to support monitoring compliance of the document?		
8.	**Review Date**		
	Is the review date identified and is this acceptable?	**Yes**	
9.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	**Yes**	
10.	**Equality Impact Assessment (EIA)**		
	Has a suitable EIA been completed?	Yes	

Committee Approval (insert name of Committee) Information Governance Steering Group			
If the committee is happy to approve this document, please complete the section below, date it and return it to the Policy (document) Owner			
Name of Chair		**Date**	
Ratification by Management Executive (if appropriate)			
If the Management Executive is happy to ratify this document, please complete the date of ratification below and advise the Policy (document) Owner			
Date: n/a			