NHS
Halton Clinical Commissioning Group

REMOTE ACCESS POLICY

Policy Author(s)	**STHK – Network Manager: Tony Atherton**
Accountable Manager(s)	**STHK – Director of Informatics: Christine Walters (SIRO)**
Ratified by (Committee/Group)	**NHS Halton CCG Integrated Governance Committee**
Date Ratified	**21/01/2017**
Target Audience	**All staff, including contractors and volunteers**
Review Date	**January 2020**

This Policy has been developed by St Helens and Knowsley Health Informatics Service (HIS), who act as NHS Halton CCG's IT Service Provider.

This policy has been approved and adopted by NHS Halton CCG and is applicable to all staff, including contractors and volunteers.

VERSION HISTORY

Issue Date	Version No	Brief Description of Change	Changed by
19/06/2013	2	Updated	STHK

St Helens and Knowsley Teaching Hospitals NHS Trust

Remote Access Policy
Version 3

The Remote Access Policy is meant to ensure the integrity and privacy of the Trusts data and information systems.

DOCUMENT NUMBER	**STHK0561**
APPROVING COMMITTEE	IG Steering Group
DATE APPROVED	January 2017
DATE IMPLEMENTED	January 2017
NEXT REVIEW DATE	Every 3 years , January 2020
ACCOUNTABLE DIRECTOR	Christine Walters, Director of Informatics
POLICY AUTHOR	Tony Atherton, Network Manager
TARGET AUDENCE	All Staff
KEY WORDS	Remote Access, STHK VPN, N3 Session, Access Restriction, Access monitor, Audit Life Cycle

Important Note:

The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as “uncontrolled” and, as such, may not necessarily contain the latest updates and amendments.

Contents

1 SCOPE

This policy applies to all equipment that is owned, leased, operated, or maintained by the St Helens and Knowsley Heath Informatics Service (STHKHIS) as well as members of staff and all third party organisations, and their employee's/contractors that access the Trust infrastructure remotely.

2 INTRODUCTION

St Helens and Knowsley Health Informatics (STHKHIS) is committed to ensuring the privacy of the Trust, its employees, and protecting its partners from unauthorised, illegal, and malicious actions by individuals and/or organisations, intentionally or otherwise. It is therefore essential that Remote access to all operational devices and/or systems is conducted through a robust framework that ensures that:

- Access is permitted through a mechanism that ensures appropriate controls are in place to restrict access to authorised staff members and third party organisations /contractors only;
- Any changes that are conducted are done so in accordance with the Trust Change Advisory Board's Procedures.
- There is a robust accountability framework present.
- The STHKHIS recommends the use of its VPN when possible for accessing Trusts resources from off site.
- Workstation security is the responsibility of both STHKHIS support personnel and the user of the remote access service.

3 STATEMENT OF INTENT

The guidelines in this policy exist to protect the Trust and its employees. This policy applies to all staff, student, temporary employees, and other personnel in or out of the Trusts premises, including employees of affiliated third-party organisations. This policy applies to all equipment that is owned, leased, operated, or maintained by the STHKHIS.

4 DEFINITIONS

Network/Operational Device: Any item that forms part of the infrastructure of the Trust network, this includes servers, routers, firewalls and PC's. This list is intended as a representative sample and is not exhaustive.

Sensitive Data: Sensitive data is defined as either personal data, as defined by the Data Protection Act 1998, or Trust proprietary information.

Remote Access: For the purposes of this document, remote access is defined as any form of access obtained from an external location and a device not connected directly to the Trust IT network.

Approved Connections

- STHK VPN
- N3 Connection

5 DUTIES ACCOUNTABILITIES AND RESPONSIBILITIES

5.1. Chief Executive

The Chief Executive as the Accounting Officer for the Trust has ultimate responsibility for ensuring that this Policy is implemented.

5.2. The Senior Information Risk Owner (SIRO)

The Director of ICT is the designated SIRO for the Trust and will be accountable for the delivery of this Policy and related work programmes;

5.3. Health Informatics Service (STHK-HIS)

- The Health Informatics Service must approve all remote access accounts.
- Manage Risk from STHK Staff and Third Party Access;
- Ensure a secure Technical Environment through the control of access;
- Manage the connection life-cycle;
- Restrict access to authorised parties only;

5.4. All Staff

Must apply to the Health Informatics Service to get a remote access VPN token (Hardware or Software), it is the responsibility of employees with remote access privileges for STHKHIS resources to ensure that their remote access connection is given the same consideration as on-site users as they are circumscribed by policy from the HIS department.

5.5. Third Party Organisation

- It is the responsibility of all third party organisations to:
- Abide by the controls detailed within this document;
- Sign and comply with the Non-Disclosure Agreement;
- To comply with the standards detailed within the Trust Network & Information Security Risk Policy and to ensure that a robust information security infrastructure is implemented and adhered to within their own organization;
- To ensure that each access session is used solely for the agreed purpose for that connection.

6 PROCESS FOR IMPLEMENTING THIS POLICY DOCUMENT

6.1. Policy Specific Procedures

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use which has to be abided by users of STHK remote access services.

6.2. Internet Security Application

All hosts that are connected to STHKHIS resources on the Trusts network via remote access technologies must use the most up-to-date internet security software; this includes Anti-Virus, Firewalls etc.

6.3. System Security Patches

The most recent security patches must be installed on the devices using the remote access connection.

6.4. Administrator right

Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Systems administration staff may have a need to disable the network access of a host if that host is disrupting production/operation services.

6.5. Acceptable User Behaviour

Under no circumstances is an employee of the Trusts or third party organisation /contractors authorised to engage in any activity that is illegal under law while utilising the STHKHIS-owned resources.

Employees and contractors with remote access privileges must ensure that their computer or workstation, which is remotely connected to Trusts resources on the Trusts network are under their complete control.

Computer facilities must only be used for authorised business. Non-business or unauthorised personal use by staff without management approval will be regarded as possible cause for disciplinary action by that organisation.

Employees and approved Trust contractors with remote access privileges must ensure that private computers (i.e. not owned by the Trust) are not connected to the Trust Network. Only computers supplied by the Trust are to be connected.

Employees and contractors with remote access privileges must ensure that their computer (owned by the Trust), that they are brought back to the Trust and connected directly to the network, at least every 3 months, to ensure any out of date patches, cached process, etc. are updated. Failure to comply could result in the asset being removed and will be regarded as possible cause for disciplinary action by that organisation.

6.6. Third Party Access Sessions

Internal session requests; All 3rd party access sessions must be logged as a call with the service desk by the individual who will be managing that particular access session. When a member of staff requires a third party to connect, a call must be logged with the service desk by the originator and the appropriate change management procedures must be adhered to. Appendix C is an example of a change management form.

6.7. Change Management

If the session is related to a change, as defined by the Change Management Policy, approval must be obtained from change management process and the session inserted into the Forward Schedule of Change.

6.8. Restriction of third Party Access – authorised personnel

The third party will ensure that the authorised personnel are appropriately trained for providing the remote service and a Non-Disclosure Formed signed (see Appendix B)

6.9. N3 Sessions

It is accepted that there is a requirement for certain third parties to access the Trust infrastructure via an N3 connection; these organisations are bound by the terms of this document.

Any remote access to the Trust infrastructure will be via a secure Virtual Private Network (VPN) and the use of a security token (Hardware or Software), a connection to the Trust network will then be established with all traffic passing through the Trust firewall. Exemption for connection via the N3 network

6.10. Access Restrictions

Any staff / third party access session MUST only occur when prior approval has been provided by the Trust. Unauthorised access may result in further action being taken against the third party, and member/s of Trust staff, in question.

6.11. Access Monitoring:

Each remote access session must have a member of the appropriate Trust team monitoring the activity of the third party. In the event of the third party accessing sensitive data, a recording of the session will be maintained. Failure to comply with this requirement may result in disciplinary action.

6.12. Termination of Access

The Trust reserves the right to terminate any remote access session without prior notice. Access may also be terminated if an unauthorised session is detected. These sessions will be terminated as soon as it is established that there will be no adverse impact upon the system that is currently being accessed.

6.13. Outbound Communications

It is accepted that during a physical visit to the site, there may be a requirement for a third party to remotely connect to their organisations network whilst connected to a Trust device. Any such connection will be bound by the contents of this policy in a non-disclosure agreement (a copy of which is enclosed in Appendix B), and it is incumbent upon the third party that there is adequate security architecture in place.

6.14. Audit Lifecycle

All remote access sessions will be subject to a full and comprehensive audit trail.

6.15. Reports

Reports will be produced on a regular basis in order to facilitate audit requirements. These reports will be stored for an appropriate period of time to ensure that they are available in the event of an incident.

6.16. Contractual Obligations

Any third party requiring remote access to Trust systems must sign and abide by one of the following document:

1. Non-disclosure Agreement

Failure to sign and comply with the requirements of these documents will prevent access from being obtained by the Third Party. Non-Disclosure Agreement (NDA). These documents may be substituted with other formal documents providing that they match the Trust's requirements. For further information, please contact the Information Governance Team. All agreements will be reviewed on a regular basis to ensure that they are both accurate and appropriate. A physical copy of the agreement will be retained by both the third party and the Trust.

6.17. Phase outs:

It is accepted that third party services were used for remote access operations on the Trust networks; such services must be gradually phased out without causing failures to critical system or business process. All new site or clients should be restricted to the approved connection services used for remote access operations as stated by this policy.

7 TRAINING

The HIS recognises that to gain the commitment of staff to support and meet local security requirements they must be aware of and understand why various procedures are in place.

- IG Training detailing the security of systems will be provided during mandatory training.

- IT training for system access will be provided by the HIS IT trainers if required.

Staff responsibilities for preservation of confidentiality, Data Protection and security must be identified in the Trust's contracts of employment and terms and conditions and should be reinforced in local induction and subsequent training in Information Governance standards.

The Trust will ensure that all users of the network are provided with the necessary security guidance and awareness via global emails to discharge their security responsibilities.
All users of the network will be made aware of the contents and implications of this Policy and (where appropriate) security procedures.

8 MONITORING COMPLIANCE WITH THIS DOCUMENT

Key performance Indicators of the Policy

Describe Key Performance Indicators (KPIs) Must reflect	Frequency of Review	Lead
Duties are carried out as described in the policy	Annually	IG Manager
Compliance will be monitored via the Information Governance Toolkit	6 Monthly	IG Manager
External Audit Rating to be of an acceptable standard.	Annually	IG Manager

Performance Management of the Policy

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
Refer to KPIs	Spot checks Website Feedback Mandatory Training IG Toolkit Reports	IG Manager	As Above	IG Steering Group Risk Management Council Trust Board	Risk Management Council Trust Board

	External Audit Reports				
IG Mandatory Training	Training will be monitored in line with the Induction Mandatory and risk Management Training Policy.				

9. RELATED TRUST POLICY/PROCEDURES

This policy should be read in conjunction with other relevant Information Governance policies, in particular:

- Information Governance Policy;
- Confidentiality Code of Conduct
- Mobile Device Policy;
- Network and Information Security and Risk Policy

These and other policies ensure the Trust complies with relevant laws and NHS guidance, including:

- Copyright, Designs & Patents Act 1988;
- Access to Health Records Act 1990;
- Computer Misuse Act 1990;
- The Data Protection Act 1998;
- The Human Rights Act 1998;
- Electronic Communications Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000;
- Health & Social Care Act 2001;
- NHS Confidentiality Code of Practice;
- NHS Information Security Code of Practice.

APPENDIX A

Equality Analysis

"St Helens and Knowsley Teaching Hospitals NHS Trust is committed to creating a culture that promotes equality and embraces diversity in all its functions as both an employer and a service provider. Our aim is to provide a safe environment, free from discrimination, and a place where all individuals are valued and are treated fairly. The Trust adheres to legal requirements and seeks to mainstream the principles of equality and diversity through all its policies, procedures and processes.

The Trust takes a zero tolerance approach to all forms of discrimination, harassment and victimisation and will make every effort to ensure that no patient or employee is disadvantaged, either directly or indirectly, on the basis that they possess any of the "protected characteristics" as defined by the Equality Act 2010 . The protected characteristics are as follows: - race; disability; sex; religion or belief; sexual orientation; gender reassignment; marriage and civil partnership; pregnancy and maternity; and age.

This policy will be implemented with due regard to these commitments.

All authors of policy documents must include a completed equality analysis Stage 1 screening. Policy authors must refer to the Trust Equality and Diversity Policy 2011 and the equality analysis toolkit and associated guidance documents (Stage 1 and Stage 2) available on the intranet.

Equality Analysis for this policy

Equality Analysis Stage 1 Screening		
1	Title of Policy:	Remote Access Policy
2	Policy Author(s):	Tony Atherton
3	Lead Executive:	Christine Walters
4	Policy Sponsor	Phil Corrin
5	Target Audience	All staff
6	Document Purpose:	
7	Please state how the policy is relevant to the Trusts general equality duties to: • eliminate discrimination • advance equality of opportunity • foster good relations	**N/A**

8	List key groups involved or to be involved in policy development (e.g. staff side reps, service users, partner agencies) and how these groups will be engaged	Trust communication tools (Team brief, global emails)

NB Having read the guidance notes provided when assessing the questions below you must consider;

- Be very conscious of any indirect or unintentional outcomes of a potentially discriminatory nature
- Will the policy create any problems or barriers to any protected group?
- Will any protected group be excluded because of the policy?
- Will the policy have a negative impact on community relations?

If in any doubt please consult with the Patient and Workforce Equality Lead

9	Does the policy **significantly** affect one group **less** or **more** favourably than another on the basis of: answer 'Yes/No' (please add any qualification or explanation to your answer particularly if you answer yes)		
		Yes/No	**Comments/ Rationale**
	• Race/ethnicity	N	
	• Disability (includes Learning Disability, physical or mental disability and sensory impairment)	N	
.	• Gender	N	
	• Religion/belief (including non-belief)	N	
	• Sexual orientation	N	
	• Age	N	
	• Gender reassignment	N	
	• Pregnancy and Maternity	N	
	• Marriage and Civil partnership	N	
	• Carer status		
10	Will the policy affect the Human Rights of any of the above protected groups?	N	
11	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	N	
12	If you have identified a negative impact on any of the above-protected groups, can the impact be avoided or reduced by taking different action?	N	

13	How will the effect of the policy be reviewed after implementation?	**NA**
If you have entered yes in any of the above boxes you **must** contact the Patient and Workforce Equality Lead (ext. 7609/ Annette.craghill@sthk.nhs.uk) to discuss the outcome and ascertain whether a **Stage 2 Equality Analysis Assessment** must be completed.		
Name of manager completing assessment: (must one of the authors)		Tony Atherton
Job Title of Manager completing assessment		Network Manager
Date of Completion:		

The Trust has a duty as a public body to publish all completed Equality Analysis Screening and Assessments. Please forward a copy of your completed proforma to Annette.craghill@sthk.nhs.uk

The Patient and Workforce Equality Lead will conduct an audit on all completed Screening and Assessments every six months.

APPENDIX B

Agreement outlining the personal responsibility concerning the security and confidentiality of information relating to service users, employees and the business of St Helens & Knowsley Teaching Hospitals Trust by staff who are not directly employed by the Trust

During the time you are working in the ……Department within St Helens & Knowsley Teaching Hospitals Trust you may come across or be asked to work with confidential information regarding service users or employees of the Trust. Under the Data Protection Act 1998 you are bound to keep such information confidential.

The Data Protection Act 1998 regulates the use of personal information and includes the electronic and paper records of service users and employees. St Helens & Knowsley Teaching Hospitals Trust is registered in accordance with this legislation. If you are found to have used any information you have seen or heard whilst working within the Trust, other than in the legitimate pursuit of your duties, you may face legal action.

Unauthorised disclosure/misuse of such information will be considered gross misconduct and will be subject to penalties under the Criminal Justice and Immigration Act 2008

Confidential information includes information relating to the business of St Helens & Knowsley Teaching Hospitals Trust.

If a breach of service user, employee, personal identifiable information, or confidential business information and/or, security and/or, a complaint of such occurs, you must immediately inform the Information Governance Manager, Information Security Officer or Caldicott Guardian.

These responsibilities are required in perpetuity and not just for the length of time you work within St Helens & Knowsley Teaching Hospitals Trust and will be relevant to your working day and outside of working hours.

I understand that I am bound by the duty of confidentiality and agree to adhere to all guidance on confidentiality given by St Helens & Knowsley Teaching Hospitals Trust.

I understand my personal responsibilities to comply with the requirements of the Data Protection Act 1998.

I am aware of the contents and implications as well as the security procedures and guidance of this Policy.

SURNAME…….FORENAME(s)…….

DESIGNATION……..ORGANISATION……..

SIGNATURE……..DATE……..

APPENDIX C

Change Management - *Request for Change*

- http://rfc.shk.nhs.uk/SitePages/Home.aspx