East London
NHS Foundation Trust

Remote Access Policy

Version number :	2.3
Consultation Groups	Digital Network and Service Delivery teams
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	24th November 2021
Name of originator/author:	Kashif Ghafoor
Executive Director lead :	Philippa Graves
Implementation Date :	November 2021
Last Review Date	November 2021
Next Review date:	November 2024

Services	Applicable
Trustwide	X
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
0.1		Daniel Woodruffe	Draft	Initial draft for comment & discussion.
1.0		Daniel Woodruffe	Final	Working draft pending approval by IGSG
2.1	March 2012	Daniel Woodruffe	Final	Annual review – March 2012 Daniel Woodruffe
2.2	February 2014	Daniel Woodruffe	Final	Review – February 2014. Daniel Woodruffe
2.3	March 2016	Simon Labonte	Final	Review – March 2016. Simon Labonte
2.4	May 2021	Alison Naughton	Final	Review – May 2021 – Alison Naughton & John Morrison
2.5	June 2021	Kashif Ghafoor	Final	Review

Introduction

This policy covers the use of the Remote Access system provided by East London NHS Foundation Trust. It should be read in conjunction with to the Internet and Email Usage Policy; the Information Governance and IM&T Security Policy and the Remote Access user instructions.

The Remote Access system allows authorised staff access to Trust systems (Intranet, email, shared files and Clinical & Managerial Systems) remotely via the Internet. The system allows access from any internet connected PC or a wifi enabled laptop (e.g. in partner agencies' sites, Local Authority offices, other NHS sites) – referred to as a "Host PC".

Great care needs to be taken when accessing systems and data from any non-Trust computers, and this policy sets out and clarifies the responsibilities of system users.

Note also that the service is designed to work with IBM compatible PC's and will not necessarily work on other formats (e.g. Apple Mac)

Eligibility

East London Foundation Trust staff may apply for Remote Access on the following conditions:

1. They are a full time member of staff and are on the Trust payroll
2. Staff have a valid network username and password, and a Trust email account
3. A request is completed, and approval is granted from the relevant Clinical or Borough Director on the IT Servicedesk Portal
4. Staff have read and acknowledged the relevant policies and agree to be bound by those policies.
5. Staff agree to monitoring of their Remote Access and to random spot checks on this access in order to ensure compliance with policy.

Registration

All remote users must be registered and authorised by the Head of IT. User identity will be confirmed by strong authentication and User ID and password authentication. The IT Service Desk and Infrastructure teams are responsible for ensuring a log is kept of all user Remote Access requests.

Responsibilities of users and key risks

Users must never disclose their network username, password or personal PIN number to anyone. Users should be vigilant when entering their personal PIN and password in a public place.

Establishing support arrangements for software on non-Trust Host devices is the responsibility of the user. No support is either provided by the Digital department or the helpdesk

In the event that a user does not own a Trust mobile phone they will be allowed to use their own personal mobile to download and receive RSA tokens.
The Digital Department is not responsible for the support of the person's personal mobile phone and can only advise on the process of downloading the relevant application.

In order to use a personal mobile phone, the user must have the most up to date version of android or IOS e.g. Android version 6 or IOS version 11.0

- Set an inactivity timeout to lock the screen e.g. 2 minutes.
- Set a PIN (fingerprint etc.) to unlock the device and do not share your PIN with anyone.
- Do not store the PIN for RSA (or anything else) on your device
- Do not use a device you share with others
- Keep the device firmware updated within 30 days of a new release
- Don't use a device for which you can no longer download firmware updates
- Do not root or jailbreak the device
- Keep ALL apps updated within 30 days of a new release – or remove the app
- Delete unsupported apps
- Do not allow anyone to use your device unsupervised
- If you lose the device, or believe it has been compromised change your passwords and monitor for unusual transactions on your bank account
- If the device has RSA SecurID, NHSMail, patient data (e.g. phone number) etc. and you believe it has been compromised or lost let the IT Service Desk know

The Digital Department is not responsible for the support of non-trust ICT equipment PCs, Broadband routers, Broadband Telephone lines and can only offer advice. The IT Service Desk will not be able to assist with any technical issues relating to staff's own, or another organisation's equipment, network or internet connection. Up to date anti-virus software and a personal firewall must be installed on all Host PC's to allow full access to the system. The Digital department does not supply this software or the configuration of these on non-Trust Host PC's. Assistance in ensuring anti-virus software is up to date and firewall is installed can be obtained from 3rd party sources or the provider of the Host PC (e.g. the local authority IT Department). It is the user's responsibility to ensure such antivirus and personal firewall software is installed and up to date before accessing the service. Failure to do so will result in a restricted service or no access at all.

Users must treat the Remote Access system as though they were using trust systems from their desktop. Users must be particularly careful when accessing sensitive information in public places (e.g. a library) and in particular: -

- Not allow others to view screen contents
- Not downloading person identifiable/confidential/sensitive data to local storage or removable media.
- Not printing person identifiable / confidential / sensitive data

Failure to follow this guidance could result in disciplinary action.

Opening up the Trust network to outside access inevitably requires additional security controls and the Trust has invested in services that provide as much protection as possible. There are, however, a number of risks users of the system should be aware of, and actions which should be taken to avoid occurrence of security incidents:

1. **Loss/theft of mobile phone.** Your mobile stores your RSA token – you should minimise the effect of any loss/theft by:
    a. Memorising your 4-digit PIN code
    b. Reporting any loss or theft immediately to both the IT department and to the Assurance Department (through the Trust's incident reporting process)

2. **Risk of 'data leakage' from the Trust.** Users of the system should not download and save any person identifiable/sensitive/confidential information to the C: drive of ANY PC/laptop or ANY removable media device. Any **non-sensitive** documents can be saved to One Drive or a local hard drive for the purposes of modification and then saved back to One Drive or a secure Trust drive (H: , I: etc.). Any documents modified on a non-Trust PC should be deleted at the end of the work session i.e. not saved permanently on the non-Trust device.

3. **Risk of unauthorised access.** Any staff member accessing the Remote Access system does so with the condition that they do not share their login with another individual. It is a disciplinary offence to allow someone else to use your login.

The Trust's IT Manager is responsible for the local definition of network, infrastructure and PC information security requirements and for the supply and configuration of all computing equipment provided by the organisation. This will include network connectivity and support for approved services.

Where, exceptionally, agreement is provided that a user may use their personal computing resources for a business purpose of the organisation, the IT manager/IM&T Security Officer must be satisfied that the resources concerned are configured appropriately, that the security measures are implemented and operating correctly and that no unacceptable information governance risks exist.

Where the proposed working arrangements involve the use of personal or shared computing resources, it must be noted the IG risks of doing so may outweigh any operational advantage. For all scenarios, consideration of risks must be made and should take account of the potential to:

- accidentally breach patient confidentiality.
- disclose other sensitive data of the organisation to unauthorised individuals.
- loss or damage critical business data.
- damage the organisation's infrastructure and e-services through spread of un-trapped malicious code such as viruses.
- create a hacking opportunity through an unauthorised internet access point.
- misuse data through uncontrolled use of removable media such as digital memory sticks and other media.
- Cause other operational or reputational damage.

All incidents involving the use of remote working facilities must be reported to the organisation's head of IT and the Head of Information Governance immediately and in accordance with the organisations incident reporting procedures.

Any comments or queries regarding the use of Remote Access should be forwarded to the Head of IT.

The Trust will undertake audits and reviews of the Remote Access Service use.

Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.