

Remote Access Policy

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 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 RiO) remotely via the Internet. The system allows access from any internet connected PC (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 form is completed, and approval is granted from the relevant Clinical or Borough Director via email to the Head of ICT.
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 ICT. User identity will be confirmed by strong authentication and User ID and password authentication. The Trust's Network Manager is responsible for ensuring a log is kept of all user Remote Access.

Responsibilities of users and key risks

Users must never disclose their network user name, 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 PCs is the responsibility of the user. No support is either provided by the ICT department or the helpdesk

The IT Department is not responsible for the support of non-trust ICT equipment - e.g PCs, , Broadband routers, Broadband Telephone lines and can only offer advice. The ICT 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 connections.

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 ICT 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 ICT Department). It is the users 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.

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 one time use code – you should minimise the effect of any loss/theft by:
 - a. Memorising your 4 digit PIN code and deleting the text message containing this code (it is not necessary to delete your 10 digit one-time use code)
 - b. Reporting any loss or theft immediately to both the ICT 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 a local hard drive for the purposes of modification and then saved back to a secure Trust drive (H:, P:, 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 virus infection.** The Remote Access system is configured so that it does not accept connections from PCs without up-to-date anti-virus software installed. You may therefore be unable to use the system if the PC you are using does not have an approved and up-to-date anti virus product installed. There can be no exceptions to this rule, as one unprotected PC gaining access to the network could put the whole Trust at risk of virus infection.
4. **Risk of unauthorised access.** Any staff member accessing the Remote Access system does so on 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.

All staff who are permitted to use their personal computing resources to connect to networked services of the organisation are subject to the requirements of this policy.

The Trust's ICT 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 ICT 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;
- lose 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 ICT 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 ICT.

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

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

East London Foundation Trust Remote Access request form

Please complete the form below to request Remote Access to the Trust's IT network.
All requests MUST be approved by the relevant Service or Clinical Director.

Name:	
Job Title:	
Directorate:	
Base location:	
Mobile Phone no:	
Director of service:	
Please explain the reason for this request, the benefits Remote Access will bring to your role and any consequences of not proceeding with this request:	

Note: The ICT department monitor all usage at a Trust wide level, and any breach of the relevant policies will be notified to the Director of IM&T for further action.

Once complete please submit this form via email to the Service/Clinical Director who has agreed to authorise your request.

All requests should then be submitted by the relevant service director to the Trust's Head of ICT or the Director of Information - via email.

Any requests not submitted by the relevant director will be returned, un-actioned.

Submission of this request constitutes an agreement by the user to abide by usage principles and conditions set out in this policy.