Tees, Esk and Wear Valleys
NHS Foundation Trust

Network User Access Procedure

Ref IT-0004-v7

Status: Approved
Document type: Procedure

Contents

1 Purpose

Following this procedure will help the Trust to:-

- Provide clear instructions and guidance on the proper use of the trust's information technology (IT) network, including gaining access to the network, and to ensure staff are aware of what is acceptable and unacceptable use.

2 Related documents

This procedure describes what you need to do to implement the 3.1 section of the Access to Information Systems Policy

The Access to Information Systems Policy defines access regulations and procedures which you must read, understand and be trained in before carrying out the procedures described in this document.

This procedure must be read in conjunction with the following policies / procedures:-

- Access to Information Systems Policy
- Information Security and Risk Policy
- Email Policy
- Internet Policy
- Data Management Policy
- PARIS Procedure

This procedure also refers to:-

- ✓ Network and Paris Request Form
- ✓ Network Account Amendment Forms
- ✓ PARIS Account Amendment Forms
- ✓ Removal of Access Forms
- ✓ Additional Network Access Form

3 Access to the Trust's computer network

3.1 Access to the network

Access to the Trust's network is via a secure logon procedure designed to minimise the opportunity for unauthorised access. Access rights are allocated on the requirements of a staff member's job description and can only be authorised by the person's line manager.

Access to **PATTI** and **Businet Networks** are not covered by this document. Guidance is outlined within the Access to Information Systems Policy.

3.2 Gaining access to the network

Once staff members are recruited in ESR, they will be given automatic access to Datix, IIC and Locality Shared Drive. All new starters to the trust and staff returning to the trust after an absence of more than 12 months **MUST** read the Network Access e-learning as soon as they log-in to the trust's network - and **BEFORE** they access any of the trust's systems, e.g. Paris. All staff must complete the Network Training Course within 5 working days of their start date

On their first login attempt the staff member will be prompted to confirm that they have read and accept Trust policies, procedures, good practices related to information security and associated information systems. They will be unable to access the Trust's network until they have confirmed this.

Once confirmed, the staff member will then log on and change their password. After the password has been changed they will then be prompted to update their contact details.

Network accounts inactive for more than 90 days will be locked by the Information Service Desk for security reasons. Users will be required to contact the Information Service Desk to go through verification and re-enable their account. If a member of staff has been absent from work, or does not use their account for over 12 months, they must re-attend network training before they can regain access to the Trust's network.

Access to NHSmail, Paris, Healthroster, Employee online and specific team shared drives must be requested via the One Form. It is the manager's responsibility to ensure the level of access requested is appropriate for the role and position of the staff member

The ONEform can be found here: One Form

3.3 Amending user accounts

Circumstances in which amendments may be needed include;

- staff changing roles on a permanent or secondment basis,
- moving to a different location, or
- making any other significant change that affects their use of the computer network e.g. change of name.

Requests to amend existing user accounts should be made by the line manager using the Amendment Section of the Oneform and sent to the Information Service Desk.

Amendments to a user's PARIS account must be requested using the PARIS Account Amendment section of the Oneform.

3.4 Removing user accounts

When a staff member has left / is leaving the Trust, their line manager should make the request to remove the user account by completing the *Leavers Section of the Oneform* and sending it to the Information Service Desk. The Service Desk will disable the user account and data will be stored within the staff member's home drive for 3 months. During this time, the line manager has the opportunity to request access to this data by completing an Additional Network Access Form. After 12 months the information is archived.

In urgent cases (e.g. where a user leaves the Trust under disciplinary circumstances) the line manager must contact the Information Service Desk immediately so the account removal process can be started.

Failure of line managers to inform the Information Service Desk when staff accounts are no longer required is a security risk and increases the likelihood of unauthorised access to the Trust's computer network.

3.5 Temporary staff and third party access

The procedures for adding, amending, and removing user accounts for temporary staff (e.g. staff on fixed-term contracts and personnel supplied through an agency) are the same as the above with the following exceptions:

- Where a manager expects a temporary person who has left the Trust to return within three months (i.e. the person is someone the Trust uses regularly) the Information Service Desk is able to temporarily disable the account and then re-enable it on return of the individual. It is the manager's responsibility to inform the Information Service Desk of this.

- Approved third party organisations may access the Trust's computer network for maintenance and support purposes once they have completed network training.

- All user accounts created for use by third parties must be disabled when not in use. When the account is in use, an appropriate member of Trust staff must supervise the third party for the duration of the work.

- The person who will supervise the third party must complete the request form on behalf of the third party; and ensure that all information security standards are adhered to. Further guidance on this section can be sought from the Information Service Desk.

Managers, at times, may need temporary user accounts urgently and in these exceptional circumstances the information department may overbook training sessions and endeavour to provide a quicker response to the request. The Head of Information Services will approve this but line managers must ensure that the necessary paperwork is submitted prior to the training taking place.

3.6 Third party access via non-trust locations using My Desktop

Third Party Access to trust systems, via a non-trust location can be available via **My Desktop**. MyDesktop allows you to remotely access a TEWV virtual desktop session from your home PC, tablet or from another organisation. From here you will be able to access your home/shared drives, InTouch and applications such as Microsoft Office and Paris.
Some functionality may be limited with regards to access of ESR, local USB devices and printing.

3.7 Permission to Use My Desktop

If you try to use MyDesktop without the Trust's permission, the Trust may prosecute you under the Computer Misuse Act 1990. The Trust monitors the use of MyDesktop and its computer network and the data stored on it. By logging on to MyDesktop you are confirming that:

- You have read, understood and agree to abide by the Trust's information policies and procedures.
- You understand that disclosing your password or not following these policies and procedures could result in disciplinary action.
- You are aware that filtering and monitoring systems are in place to control the use of the email system and access to the internet.
- You are aware that Paris is an audited system and that you should only access patient records in accordance with Trust policies and procedures

Tees, Esk and Wear Valleys NHS Foundation Trust cannot guarantee you will be able to access MyDesktop whilst using 3rd party devices or connections. You must first check with the person or organisation that is responsible for supporting the device, that it is capable of accessing https://mydesktop.tewv.nhs.uk .Any 3rd party policies or procedures should also be adhered to, in addition to the policies and procedures of Tees, Esk and Wear Valleys NHS Foundation Trust when using MyDesktop.

4 Definitions

Term	Definition
Network	• A collection of communication equipment such as servers, computers, printers and other IT devices which have been connected together usually by cables. The network is created to share data, software and peripherals such as printers, tape drives, connection to the internet and other data storage equipment.
Authorised users	• Individual's (staff and non-staff) who have been validated and approved by the trust to use its computer network and associated information resources.
User Accounts	• Defines the actions and privileges an authorised user has in terms of accessing the Trust's network.
My Desktop	• Defines the system used for 3rd parties to access trust systems via non-trust sites and devices

5 How this procedure will be implemented

- This procedure will be published on the Trust's intranet and external website.
- Line managers will disseminate this procedure to all Trust employees through a line management briefing.

5.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	E-Learning	45-60 minutes	Part of Induction Procedure

6 How the implementation of this procedure will be monitored

Auditable Standard/Key Performance Indicators		Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	No. of new network accounts created	Monthly / Information Service Desk Supervisor	
2	No. of accounts disabled	Monthly / Information Service Desk Supervisor	
3	No. of accounts created for My Desktop system	Monthly / Information Service Desk Supervisor	
4	No. of Network training packages completed	Monthly / Supporting Users	

7 References

Guidance on completion of Network and Paris account request process

8 Document control

Date of approval:	03 October 2018	
Next review date:	31 October 2023	
This document replaces:	Network Access and User Operational Procedure IT/0004/v6	
Lead:	Name	Title
	Craig Etherington	Interim Service Desk Manager
Members of working party:	Name	Title
	John Mackay Chris Stainsby	Service Desk Team Lead Technology Officer
This document has been agreed and accepted by: (Director)	Name	Title
	Patrick McGahon	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Information Governance Board	03 October 2018
An equality analysis was completed on this document on:	07 August 2018	

Change record

Version	Date	Amendment details	Status
7	10 Oct 2018	Updated Template Updated hyperlinks for One form and procedures Addition of My Desktop section / links	Published
	July 2020	Review date extended 6 months	
	Oct 2022	Review date extended to 30 April 2023	
	Aug 2023	Review date extended to 31 Oct 2023	

Appendix 1 - Equality Analysis Screening Form

Please note; The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Service Desk, Information Department						
Name of responsible person and job title	Craig Etherington, Interim Service Desk and Technology Manager						
Name of working party, to include any other individuals, agencies or groups involved in this analysis	Craig Etherington, Chris Stainsby, John Mackay, Andrea Shotton						
Policy (document/service) name	Network User Access Procedure						
Is the area being assessed a…	Policy/Strategy		Service/Business plan		Project		
	Procedure/Guidance				Code of practice		
	Other – Please state						
Geographical area covered	All trust staff and 3rd parties accessing trust networks						
Aims and objectives	Provide clear instructions and guidance on the proper use of the trust's information technology (IT) network, including gaining access to the network, and to ensure staff are aware of what is acceptable and unacceptable use						
Start date of Equality Analysis Screening (This is the date you are asked to write or review the document/service etc.)	31 July 2018						
End date of Equality Analysis Screening (This is when you have completed the equality analysis and it is ready to go to EMT to be approved)	7 August 2018						

You must contact the EDHR team if you identify a negative impact. Please ring Sarah Jay or Ian Mhlanga on 0191 3336267/3046

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?

All trust staff and 3rd parties requiring access to the Trust Networks

2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?

Race (including Gypsy and Traveller)	No	**Disability** (includes physical, learning, mental health, sensory and medical disabilities)	Yes	**Sex** (Men, women and gender neutral etc.)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and philosophical belief's)	No	**Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners)	No

Yes – Please describe anticipated negative impact/s

Possible impact on users with visual impairment. In such circumstances, Managers should provide access to the Trust's Reasonable adjustment procedure via Human Resources. This can explore additional specialist hardware / software to support users.

No – Please describe any positive impacts/s

The procedure will ensure equal access for all to the trusts Network

3. Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? **If 'No', why not?**	**Yes**			

Sources of Information may include: • Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc. • Investigation findings • Trust Strategic Direction • Data collection/analysis • National Guidance/Reports		• Staff grievances • Media • Community Consultation/Consultation Groups • Internal Consultation • Research • Other (Please state below)

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Sex, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership

Yes – Please describe the engagement and involvement that has taken place

Yes – Detailed user testing and engagement was conducted as part of the 3rd party access product evaluation, prior to release. In addition evaluation of user calls received and details logged within the Trust's Service desk service desk system (Assure) have also been used to identify any required changes to procedures.

No – Please describe future plans that you may have to engage and involve people from different groups

Assure calls will continue to be monitored and evaluated as part of the ongoing procedures

5. As part of this equality analysis have any training needs/service needs been identified?					
No	Ongoing use of the Trust Network E-learning tools and associated guidance documents will meet current requirements				
A training need has been identified for;					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Type name: Craig Etherington				Date: 7 Aug 2018	
Your reporting (line) manager: Type name: Lorraine Sellers				Date: 7 Aug 2018	
If you need further advice or information on equality analysis, the EDHR team host surgeries to support you in this process, to book on and find out more please call: 0191 3336267/3046					

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	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.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	

7.	**Implementation and monitoring**		
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?		
Signature:			