Public – To be published on the Trust external website

Title: Network User Access Procedure

Ref: IT-0004-v8

Status: Approved
Document type: Procedure
Overarching Policy: Access to Information Systems Policy

Contents

1 Introduction

Effectively controlled access to Trust systems (by our staff and external partners) is fundamental to essential cyber security management of systems, records, and associated risks. This is recognised by the National Cyber Security Centre, and numerous sequences of the Data Security and Protection Toolkit. This procedure supports the Access to Information Systems Policy and supports the security and integrity of trust systems.

This procedure supports Our Journey To Change (OJTC) as set out in the Access to Information Systems Policy.

2 Who this procedure applies to

This procedure applies to anyone requiring access to Trust information systems, including but not limited to:

Group	Details
Staff	Employees of the trust
Service Users	Users of the Trust Services
Patients	In-patients requiring access to the internet (PATTI)
Students	Students training with or on assignment to the Trust
Volunteers	Volunteers working with the Trust
Line Managers	Managers employed by the Trust
Digital and Data Services /Service Desk	Service Desk Analysts and Officers within the Trust's Digital and Data Services
External Suppliers / Contractors	Suppliers and contractors, and their representatives, employed and authorised by the Trust
Partnership Agencies	Partnership Agencies, and their representatives, as authorised by the Trust

3 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.

- Ensure that network access is provided to only those with legitimate reason and at the appropriate level.

4 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: -

- OneForm

5 Access to the Trust's computer network

5.1 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 NHS Wi-Fi Networks are not covered by this document. Guidance is outlined within the Access to Information Systems Policy.

5.2 Gaining access to the network

Once staff members are recruited in ESR, they will be given access to the network and a core range Trust system.

All new starters to the trust and staff returning to the trust after an absence of more than 12 months **MUST** complete the Network Access MetaCompliance course 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 60 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 the "Network Access MetaCompliance course" before they can regain access to the Trust's network.

Access to Electronic Patient Record Systems, 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 on the trust intranet.

5.3 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.

There are circumstances where a change may be required to be confidential in these situations a request can be made directly to the Service Desk Lead or End User Computing Manager.

5.4 Removing user accounts

The Information Service Desk will receive notice that a user has left the Trust by one of the following methods:

- ESR Directory Manager leaver report (e.g., employee whose employment has ended on ESR)
- Oneform submitted by line manager (e.g., volunteer)
- Telephone call from line manager (e.g., where a user leaves the Trust under disciplinary circumstances and immediate removal is required)

The Service Desk will disable the user account, remove all associated permissions and data will be stored within the staff member's home drive for 3 months. During this time, the line manager can request access to this data by completing an Additional Network Access Form. After 12 months the information is archived. In addition, and where applicable the Service Desk will enter the leave date into PARIS to disable the account.

The Service Desk will mark the NHS mail account as a leaver. The account remains in the leaver status on the system for 30 days after which the account and the data within it will be eligible for deletion. The data within the account is retained and recoverable in line with the data retention policies for NHS mail.

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

5.5 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 person on temporary employment who has left the Trust to return within three months (i.e., the person is someone the Trust uses regularly) the Information Service Desk can 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 Digital and Data Services Department may overbook training sessions and endeavour to provide a quicker response to the request. A Head of Digital and Data Services will approve this, but line managers must ensure that the necessary paperwork is submitted prior to the training taking place.

5.6 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 **MyDesktop**. 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, Intranet and applications such as Microsoft Office and Electronic Patient Record Systems. Some functionality may be limited with regards to access of ESR, local USB devices and printing.

5.7 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 Electronic Patient Record Systems are 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 (TEWV) cannot guarantee you will be able to access MyDesktop whilst using third party devices or connections. You must first check with the person or organisation that is responsible for supporting the device, that it can access https://mydesktop.tewv.nhs.uk

When connecting to https://mydesktop.tewv.nhs.uk not only must the policies and procedures of TEWV be adhered to but any third party policies or procedures for the device you are using to connect to https://mydesktop.tewv.nhs.uk must be adhered to in addition.

5.8 Cyber Security Training

Everyone with a network account, regardless of employment status, must complete their monthly MetaCompliance training to continuously improve their understanding of cyber security awareness and risks. In addition, line managers (or equivalent) must also maintain a proper record of this training.

6 Definitions

Term	Definition
Network	• A system of connected devices that can communicate with each other and share resources such as files and printers.
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 Trust staff and third parties to access trust systems via non-trust sites and devices.

7 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.

7.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
n/a				

7.2 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	E-Learning	45-60 minutes	Part of Induction Procedure
All staff	MetaCompliance Cybersecurity e-learning	2 minutes	monthly

8 How the implementation of this procedure will be monitored

Number	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 this month	Monthly / Information Service Desk Supervisor	DPAG
2	No. of accounts disabled	Monthly / Information Service Desk Supervisor	DPAG
3	No. of accounts created for My Desktop system	Monthly / Information Service Desk Supervisor	DPAG
4	No. of Network training packages completed	Monthly / Supporting Users	DPAG
5	100% all new starters complete new starter network e-learning within five working days of joining the trust	Weekly, dashboard on iic (pulls data from AD and from ESR), service desk supervisor	DPAG

9 References

Logging into NHSmail as a new user for the first time
NHSmail Acceptable use Policy

10 Document control (external)

To be recorded on the procedure register by Policy Coordinator

Required information type	Information
Date of approval	02 January 2024
Next review date	02 January 2027
This document replaces	Network user access procedure IT-0004-v7
This document was approved by	Digital and Data Management Meeting
This document was approved	02 January 2024
This document was ratified by	n/a
This document was ratified	n/a
An equality analysis was completed on this procedure	05 December 2023
Document type	Public
FOI Clause (Private documents only)	n/a

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	Withdrawn
7	July 2020	Review date extended 6 months	Withdrawn

7	Oct 2022	Review date extended to 30 April 2023	Withdrawn
8	02 Jan 2024	Full review with text updated. Amendments to the ordering of the sections. The following new sections have been added Introduction; Who this Procedure Applies to; Cyber Security Training and Implementation Action Plan Small clarification to usage including: “Network Access Meta Compliance course”, “ESR Directory Manager”, and procedure.	Published

Appendix 1 - Equality Impact Assessment Screening Form

Please note: The Equality Impact Assessment Policy and Equality Impact Assessment Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Service Desk / Digital and Data
Title	Network User Access Procedure
Type	Procedure
Geographical area covered	Trustwide
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	May 2023
End date of Equality Analysis Screening	25 Aug 2023

Section 2	Impacts
Who does the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	All trust staff and third parties requiring access to the Trust Networks
Will the Policy, Procedure, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups? Are there any Human Rights implications?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO.** • **Sex** (Men and women) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women / people who are breastfeeding, women / people accessing perinatal services, women / people on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO** • **Human Rights Implications NO** (Human Rights - easy read)
Describe any negative impacts / Human Rights Implications	Staff requiring reasonable adjustments to support their access to the network at TEWV can link in with the reasonable adjustments team where they will be supported through the process and access to the required equipment / software / training etc will be explored to support users.
Describe any positive impacts / Human Rights Implications	The procedure will ensure equal access for all to the Trust's Network

Section 3	Research and involvement
What sources of information have you considered? (e.g., legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	SEE REFERENCES SECTION
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes –
If you answered Yes above, describe the engagement and involvement that has taken place	Detailed user testing and engagement was conducted as part of the third 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 (ASM) have also been used to identify any required changes to procedures.
If you answered No above, describe future that you may have to engage and involve people from different groups	ASM calls will continue to be monitored and evaluated as part of the ongoing procedures

Section 4	Training needs
As part of this equality impact assessment have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

Check the information you have provided and ensure additional evidence can be provided if asked.

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 / Not applicable	Comments
1. Title		
Is the title clear and unambiguous?	Y	
Is it clear whether the document is a guideline, policy, protocol or standard?	Y	
2. Rationale		
Are reasons for development of the document stated?	Y	
3. Development Process		
Are people involved in the development identified?	Y	
Has relevant expertise has been sought/used?	Y	
Is there evidence of consultation with stakeholders and users?	Y	INFORMED BY SERVICE DESK CALLS AND FEEDBACK
Have any related documents or documents that are impacted by this change been identified and updated?	N	Access policy in the process of being updated
4. Content		
Is the objective of the document clear?	Y	
Is the target population clear and unambiguous?	Y	
Are the intended outcomes described?	Y	
Are the statements clear and unambiguous?	Y	
5. Evidence Base		
Is the type of evidence to support the document identified explicitly?	Yes	REFERENCES

Are key references cited?	Yes	
Are supporting documents referenced?	Yes	SEE RELATED DOCS
6. Training		
Have training needs been considered?	Y	
Are training needs included in the document?	Y	
7. Implementation and monitoring		
Does the document identify how it will be implemented and monitored?	Y	
8. Equality analysis		
Has an equality analysis been completed for the document?	Y	
Have Equality and Diversity reviewed and approved the equality analysis?	Y	Abigail Holder 05/12/2023
9. Approval		
Does the document identify which committee/group will approve it?	Y	ddmm
10. Publication		
Has the procedure been reviewed for harm?	Y	No harm - Anything dangerous to trust security in this doc? = no
Does the document identify whether it is private or public?	Y	public
If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	
11. Accessibility (See intranet accessibility page for more information)		
Have you run the Microsoft Word Accessibility Checker? (Under the review tab, 'check accessibility'. You must remove all errors)	Y	
Do all pictures and tables have meaningful alternative text?	Y	

Do all hyperlinks have a meaningful description? (Do not use something generic like ‘click here’)	Y	