The Tavistock and Portman
NHS Foundation Trust

Acceptable use of IT systems and information (Directorate of Education and Training)

Type	Education and Training
Version:	1.0
Bodies consulted:	AD Information Governance, Director of Quality, Director of IM&T
Approved by:	EMT
Date approved:	21 February 2022
Lead manager:	Operations Director, Education and Training
Responsible director:	Director of Education and Training
Date issued:	February 2022
Review date:	February 2024
Intranet	Yes
Extranet	Yes

Contents

Contents 2

Acceptable use of IT systems and information (Directorate of Education and Training) ... 3

1. Introduction 3
2. Purpose 3
3. Scope and applicability 3
4. Policy Statements 4
5. Exceptions to Unacceptable Use 7
6. Duties and responsibilities 7
7. Procedures 8
8. Training Requirements 8
9. Process for monitoring compliance with this policy 8
10. References 8
11. Associated documents 8
12 Equality Impact Analysis 9

Acceptable use of IT systems and information (Directorate of Education and Training)

1. Introduction

1.1. This document explains the rules that staff and students in the Trust's Directorate of Education and Training (DET) must agree to in order to access and use Trust information systems and assets, including access to information systems, whether internally or third party hosted, hardware and equipment, Intranet and email.

1.2. The document also explains the Trust's responsibilities for meeting 'Prevent' duties under Section 26 of the Counter Terrorism and Security Act 2015, and is supplementary to Trust procedures for Acceptable use of IT systems and information that is applicable to all staff.

1.3. The Trust has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism (known as the 'PREVENT duty'). termed "PREVENT". The purpose of this duty is to aid the process of preventing people from being drawn into terrorism. Act in breach of the criminal law. Being drawn into terrorism includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit.

2. Purpose

2.1. The purpose of this document is to set out the principles of acceptable use of Trust IT systems and assets, including equipment and hardware, software, and information systems and assets.

2.2. The document also sets out the requirements of schools and higher educational establishments to comply with Section 26 of the Counter Terrorism and Security Act 2015.

2.3. Staff should also be familiar with guidance for all staff on the Acceptable use of IT systems and information on the Trust's Intranet.

3. Scope and applicability

3.1. This policy covers use of Trust wide IT systems and information assets, including equipment and hardware, software, and information systems and assets.

3.2. This policy is applicable to all staff and students working or studying in the Directorate of Education and Training (DET).

4. Policy Statements

4.1 Access to Trust information systems is for Trust business or educational purposes only

a) Individuals legitimately provided with access to Trust information systems or resources must comply with the rules of acceptable use set out within these pages.

b) Access is not permitted to anyone who no longer works for or studies with the Trust. Access will be terminated by the end of the user's last working day or last date of student registration.

c) Personal confidential information about patients, staff, students or other individualsmust only be accessed or shared for Trust business purposes, that is, to enable you to fulfil the responsibilities of your role, or that is necessary to complete your education with the Trust. You must not access or share patient, student or staff information other than for these purposes.

d) Staff and clinical trainees must complete their mandatory NHS Data Security Awareness training before accessing any patient or student information system. You will not be provided with editing rights to patient or student information systems until you have completed Trust system training (e.g. Carenotes or MyTap).

e) All access may be audited.

4.2 Passwords must be kept confidential

Don't tell anyone else your password and don't write it down. Your username and password are for your use only. It is a disciplinary offence to share your password with anyone else, to log on or attempt to log on using someone else's log on credentials.

4.3 Internet is provided for business or educational purposes

a) Access to the Internet is provided for Trust business or educational purposes. Personal use is permitted providing you use the Internet responsibly and it does not interfere with your duties.

b) Use for private business activities, personal social media or personal discussion forums is not permitted.

c) Users must not use Trust systems or Internet access to obtain view or share any material which may incite hatred or violence or breaches the criminal law, encourages or promotes any acts of terrorism, or promotes individuals, groups or organisations including proscribed organisations that support terrorism within the UK or abroad,

e) Inappropriate content (including obscene or pornographic material, or material which may incite hatred or violence or beaches of criminal law, or encourage or promote acts of terrorism, or promote individuals, groups or organisations that support terrorism within the UK or abroad) must not be accessed.

f) Commercial software or licenced material must not be downloaded or installed (except by authorised staff in IT).

g) Use of Internet based file sharing applications is not permitted unless explicitly approved and provided as a service by the Trust's IM&T Department.

h) Please note: The Trust does not guarantee the security of Guest WiFi or Public WiFi. Please refer to our terms and conditions for access to the Internet via Guest or Public WiFi.

i) The Trust reserves the right to monitor all access to the Internet, including via guest or Public WiFi. If misuse is identified by a member of staff or a student, actions may be taken under the relevant disciplinary procedure (see section 11 on related documents). If misuse from a staff member or a student raises concerns under the Trust's PREVENT duty, the Trust's PREVENT policy and procedure must be followed, to ensure the concerns are considered appropriately.

4.4 Trust email is for Trust business purposes only

a) The Trust provides email accounts to employees, student trainees, contractors, Non-Executive Directors and other individuals who work for or on behalf of the Trust.

b) Emails are business records and may be subject to disclosure under the Freedom of Information Act or the UK GDPR (as part of a Subject Access Request). The Trust monitors email usage and reserves the right to access Trust email accounts.

c) Patient information that forms part of the care record must not be retained in email but transferred to the patient information system as soon as possible.

d) Confidential information should be sent via secure email (Cryptshare) unless patient consent has been obtained to send by standard email. Use NHSmail to share patient identifiable information with staff at other NHS organisations. Consider adding a protective marking to confidential information, in line with government classifications, so that recipients know how to treat the information (see Data Classification Policy). Follow Trust procedures for using email safely and securely, particularly when communicating externally and with patients.

e) You must not use your Trust email address for private purposes, including social media, discussion forums or signing up for newsletters. Staff must not use their private email address(es) for business purposes.

f) Users must not broadcast personal messages, advertisements or other non-business related information via Trust (or other NHS) email systems. Users must not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene, incite hatred or violence,encourage or promote acts of terrorism or promote or support terrorism in the UK.

g) If you are leaving the Trust or will be taking planned absence of longer than 90 days, please note that your email account will be disabled by 6.00 pm on your last working day. Make sure you housekeep your mailbox so that no information about patients, students or other staff is still held in your mailbox and forward any relevant business information to colleagues before you leave.

4.5 The IT Service Desk must be notified about Starters, Movers and Leavers using the correct forms.

a) Managers should make sure that they select the correct type of employment from the drop-down menu on the New User Request Form. For non-employees a contract end date is required. Access will be disabled at the end of the user's last working day unless an Amend User Request form is submitted.

b) If you are moving roles within the Trust you will keep the same email address but you should housekeep your mailbox as above so that only information pertaining to your new role remains in your mailbox.If you are leaving the Trust, please note that you will not be permitted access to Trust information systems beyond your last working day and you should ensure that all Trust equipment is returned to IM&T bythe end of your last working day. This is your responsibility and the value of any devices not returned may be deducted from your final salary.

c) As with Trust email, if you are Trust staff or a student trainee, make sure you also housekeep your NHSmail account before leaving Trust employment. If you are moving to another Trust, you will b able to retain your NHSmail email address but Trust business should be deleted from your account before your last day.

4.6 Trust IT equipment must always be protected

Trust owned IT equipment must always be protected from damage or theft.

Always keep laptops and mobile phones with you whilst travelling.

Protect equipment from environmental damage, including rain or extreme heat or cold.

Do not leave Trust equipment on display or unattended in vehicles.

4.7 Trust equipment must be returned before the user's last working day.

Trust equipment may only be used by the member of staff who has signed for and taken personal responsibility for the device.

Trust equipment must be returned to IM&T when no longer required and, if you are leaving the Trust, by the end of your last working day. This includes laptops, tablets, mobile phones, display equipment and (where relevant) printers.

4.8 Where to go for help.

If you have any questions about the rules of acceptable use of Trust IT systems, equipment or information, please ask your line manager or email the IG team at IG@tavi-port.nhs.uk.

5. Exceptions to Unacceptable Use

5.1 Exceptions to this policy

For undertaking certain activities, including for research purposes, audit or investigations, exceptions to this policy may be permitted.

In such circumstances, advice should be sought from the Trust's Information Governance lead, Adult Safeguarding and Prevent Lead or the Operations Director, Education and Training, as appropriate.

6. Duties and responsibilities

6.1 Who is covered by this policy

All Directorate staff (including employees, contractors or third parties) and students who access Trust information systems, equipment or information assets in the course of their work or education with the Trust have a duty to comply with this policy.

Non-compliance with this policy may result in disciplinary action, dismissal or exclusion, in line with the Trust's Disciplinary Procedure and /or the Trust's Prevent procedures.

6.2 If you suspect a breach

If a staff member, student, or visitor believes they may have encountered breaches of any of the above, they should make this known to the relevant lead, as above.

7. Procedures

- Acceptable use of IT systems and information (Procedures)
- Guest WiFi and Public Wi-Fi Terms and conditions of use
- Trust Prevent policy and procedure
- Communicating with patients and sharing patient information electronically

8. Training Requirements

All staff and clinical students working for or on behalf of the Trust must complete and pass their annual NHS Data Security and Awareness Training.

9. Process for monitoring compliance with this policy

Compliance with this policy will be monitored by the Trust's IMT Directorate,who will report to the Integrated Governance Committee (IGC) via the Data Security & Protection Sub-Committee.

10. References

- Counter-Terrorism and Security Act 2015 (Section 26)
- Prevent duty guidance (Home Office guidance) – for England and Wales

11. Associated documents[1]

- Data Protection Policy
- Information Governance Management Framework
- Information Security Policy
- Prevent Policy and Procedure
- Disciplinary Policy and Procedure (staff)
- Student Conduct Concerns Procedure

[1] For the current version of Trust procedures, please refer to the intranet.

12 Equality Impact Analysis

Completed by	**Will Fitzmaurice**
Position	**Operations Director, Education & Training**
Date	**27.01.22**

The following questions determine whether analysis is needed	**Yes**	**No**
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?		X
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?		X
Does the policy relate to any equality objectives that have been set by the Trust?		X
Other?		X

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then undertake the analysis below:

	~~Yes~~	~~No~~	~~Comment~~
~~Do policy outcomes and service take-up differ between people with different protected characteristics?~~			
~~What are the key findings of any engagement you have undertaken?~~			
~~If there is a greater effect on one group, is that consistent with the policy aims?~~			
~~If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?~~			
~~Will the policy deliver practical benefits for certain groups?~~			
~~Does the policy miss opportunities to advance equality of opportunity and foster good relations?~~			
~~Do other policies need to change to enable this policy to be effective?~~			
~~Additional comments~~			

If one or more answers are yes, then the policy may be unlawful under the Equality Act 2010 –seek advice from Human Resources (for staff related policies) or the Trust's Equalities Lead (for all other policies).