The Tavistock and Portman NHS
NHS Foundation Trust

Acceptable Use Procedure

Version:	V1.0
Bodies consulted:	IG Workstream
Approved by:	Executive Management Team
Date approved:	12 March 2019
Lead manager:	Data Security and Protection Manager & DPO
Responsible director:	Senior Information Risk Owner (Deputy Chief Executive & Director of Finance)
Date issued:	13 March 2019
Review date:	February 2024
Intranet	Yes
Extranet	Yes

Is this policy current? Check the intranet to find the latest version!

Contents

Acceptable Use Procedure

1. Introduction

The Tavistock and Portman NHS Foundation Trust is a specialist mental health training provider based in London with an international reputation for excellence in the mental and social care sector. The Trust is a specialist in mental health with focus on training and education alongside a full range of multi-disciplinary services for adults, adolescents and children and their families; these services cover a spectrum of psychoanalytic, psychotherapeutic and systemic approaches.

This Acceptable Use Procedure ("AUP") aims to ensure all users of Trust information management and technology (IMT) resources and services, be they staff, students, patients or members of the public, comply with the relevant laws and regulations governing use of the services, including but not limited to data security and protection regulations. IMT resources and services include, but are not limited to:

- use of Trust devices,
- access to clinical, corporate and educational systems, and
- Trust provided internet connectivity either via Trust or personal devices.

By using Trust IMT services, you acknowledge that you are responsible for your compliance with the Trust AUP.

2. Purpose

This Acceptable Use Procedure is intended to provide a framework for such use of the Tavistock and Portman NHS Foundation Trust IMT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

3. Scope

All individuals making use of Trust IMT services (staff, students, visitors, contractors and other members of the public) are bound by the provisions of the Trust Acceptable Use Procedure. The Trust seeks to promote and facilitate the positive and extensive use of Information Technology in the interest of supporting delivery of learning, teaching, innovation, services and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff, partners of the Trust.

This Acceptable Use Procedure is not taken to overrule any additional terms of use for specific systems, include those governing and user obligations such as associated Copyright Acknowledgement and General Terms of Service of the Trust and NHS systems, devices or applications deployed in support of Trust, NHS or health and social care business functions.

4. Applicability

This Procedure is applicable to and designed for use by Tavistock and Portman NHS Foundation Trust, its staff, students, patients, and visitors that have access to its systems and/or information and data at any level.

5. Guidance

This Procedure provides guidance and conditions for its use and Implementation:

Term	***Meaning/Application***
SHALL	*This term is used to state a Mandatory requirement of this Procedure*
SHOULD	*This term is used to state a Recommended requirement of this Procedure*
MAY	*This term is used to state an Optional requirement*

6. Internet Acceptable Use

The Trust provides internet access to Trust staff, third party associates, students, patients, and other members of the public via several separately secured networks including over WiFi.

- Information found on the Internet is subject to minimal regulation and as such must be treated as being of questionable quality. You should not base any business-critical decisions on information from the Internet that has not been independently verified.
- Internet access via the primary Trust infrastructure is mainly provided for business purposes. For the purpose of simplifying everyday tasks, limited private use may be accepted. Such use includes access to web banking, public web services and phone web directories.
- Excessive personal use of the Internet during working hours shall not be tolerated and may lead to disciplinary action.
- Users shall not use Internet-based file sharing applications, unless explicitly approved and provided as a service.
- Users shall not upload and download private data (e.g. private pictures) to and from the Internet.
- Users shall not download copyrighted material such as software, text, images, music and video from the Internet.
- Users shall not use trust systems or Internet access for personal advantages such as business financial transactions or private business activities.
- Users shall not use their Tavistock and Portman NHS Foundation Trust identity (i.e. using tavi-port.nhs.uk, .ac. .org e-mail address) for private purposes such as on social media, discussion forums.

- Guest WiFi provides internet access for students, patients, visitors and other members of the public. The internet access provided is subject to filtering and does not grant access to the primary Trust network or systems.

7. Guest Wi-Fi Acceptable Use

This governs the use of our guest WI-FI service by all users. It is your responsibility to ensure the appropriate use of the Trust (Tavi_Guest) guest wireless network in accordance with the following terms:

- The guest Wi-Fi access is continuously monitored and will actively prevent access to inappropriate content.
- The Trust does not guarantee the security, confidentiality or the integrity of the user's information on the guest wireless network.
- The Trust is not responsible for the loss, misuse or theft of any information, passwords or other data transmitted by users through the guess wireless network
- Access to the internet via Trust guest wireless network is monitored for inappropriate material and sites which are deemed to contain unsuitable material will be blocked
- You will not take photos of patients, visitors or staff to be uploaded onto any internet -based services without the explicit permission of that person.
- Your access to this service is completely at the discretion of the Trust and your access to the service may be blocked, suspended or terminated at any time for any reason including, but not limited to, violation of this agreement, actions that may lead to liability for Trust, disruption of access to other users or networks, or violation of applicable laws or regulations
- The Trust may revise these terms at any time and without notice. It is your responsibility to review this Procedure for any changes.

8. Trust and NHS Email Acceptable Use

- Email services within the Trust and NHS are provided for business purposes. Limited private use for the purpose of simplifying everyday tasks may be accepted but private emails should be distributed via web-based email services.
- Users shall not use external e-mail services (e.g. hotmail.com, gmail.com) for business communications and purposes.
- Private emails should be stored in a separate folder named 'Private e-mail box'. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection.
- Private emails should be deleted as soon as possible in order to limit storage requirements for non-business information.
- Users shall not broadcast personal messages, advertisements or other non-business-related information via Trust and NHS e-mail systems.
- Users shall not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene.

- Users shall not distribute statements of a political or religious nature, or other information of a personal nature.
- Engaging in any illegal activities via e-mail is prohibited. Discovery of such material shall, if deemed as being of a criminal nature, be handed over to the police.
- Patient and staff identifiable data **shall** only be sent via secure means. Guidelines for this are set out in the Data Protection Procedure and Information Governance Management Framework.

9. Use of Systems Procedure

Use of Information Systems

- *Unauthorised Information Access*

- Tavistock and Portman NHS Foundation Trust and third-party employees shall only be authorised access to information relevant to their work.
- Accessing or attempting to gain access to unauthorised information shall be deemed a disciplinary offence.
- When access to information is authorised, the individual user shall ensure the confidentiality and integrity of the information is upheld, and to observe adequate protection of the information according to Trust and NHS policies as well as legal and statutory requirements. This includes the protection of information against access by unauthorised persons

10. Misuse of Information Systems

Use of the Trust information systems for alleged malicious purposes shall be investigated in line with the Trust disciplinary procedure. This includes but is not limited to:

- Penetration attempts (“hacking” or “cracking”) of external or internal systems.
- Unauthorised electronic eavesdropping on or surveillance of internal or external network traffic.
- Discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or material on computer or communications media; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems.
- Acquisition or proliferation of pornographic or material identified as offensive or criminal.
- Deliberate copyright or intellectual property rights violations, including use of obviously copyright-violated software, content or other publications.
- Storage or transmission of large data volumes for personal use, e.g. personal digital images, music or video files or large bulk downloads or uploads.
- Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other person without a legitimate purpose and prior authorisation from senior management is strictly forbidden and shall be deemed a disciplinary offence.

- Use of Trust information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and shall be deemed a disciplinary offence.
- If identified misuse is considered a criminal offence, criminal charges shall be filed with local police and all information regarding the criminal actions handed over to the relevant authorities.

11. Guidelines for IMT Equipment Use

Physical Protection:

- Users shall not eat or drink in the vicinity of any IMT infrastructure equipment.
- Users shall not expose any IMT equipment, including personal devices, to magnetic fields which may compromise or prevent normal operation.
- Users shall not expose any IMT equipment to external stress, sudden impacts, excessive force or humidity.
- Only authorised IMT support personnel shall be allowed to open Trust IMT equipment and equipment cabinets.
- If left unattended in semi-controlled areas such as conference rooms or reception offices, laptops should be locked using the Ctrl-Alt-Delete or other applicable method.
- Portable equipment shall never be left unattended in airport lounges, hotel lobbies, cafes, Rail and Bus stations and similar areas as these areas are insecure.
- Portable equipment shall be physically locked down or locked away when left in the office overnight.
- Portable equipment shall never be left in parked cars, unless completely invisible from outside the vehicle and protected from extreme temperatures.
- Portable equipment shall not be checked in as hold luggage when travelling, but treated as hand or cabin luggage at all times

12. General Device Use

- Users shall lock their terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method) when not left unattended, even for a short period.
- Users shall not install unapproved or privately-owned software on Trust IMT equipment.
- Only authorised Tavistock and Portman NHS Foundation Trust IMT personnel shall be allowed to reconfigure or change system settings on the IMT equipment.
- Laptops and mobile devices shall:
    - Only be used by the Trust or third-party employee that has signed and taken personal responsibility for the laptop.
    - Have the corporate standard encryption software installed, rendering the information on the laptop inaccessible if the laptop is stolen or lost.

  - Have the corporate standard anti-virus, anti-spyware and personal firewall software installed.
  - Have the corporate standard remote access installed.

- If configured according to the specifications above the laptop/mobile device may be connected to wired or wireless access points.
- Trust laptops and mobile devices shall never be (via cable or wireless) directly connected to other non-Trust IMT equipment or systems.
- Users shall not use privately owned storage devices or storage devices owned by third parties for transfers of Trust data.
- Any device lost or stolen shall be reported immediately to the Tavistock and Portman NHS Foundation Trust Service Desk team.
- Users are not permitted to save personal data to the local C drive.

13. References

13.1. Computer Misuse Act 1990
13.2. Lawful Business Practice Regulation 2000
13.3. Regulation of Investigatory Powers Act 2000
13.4. Data Protection Act 2018
13.5. General Data Protection Regulation

14. Associated documents

14.1 Data Protection Policy
14.2 Information Governance Management Framework
14.3 Information Security Policy

12 Equality Analysis

Completed by	**Ndumbe Shu**
Position	**Data Security and Protection Manager & DPO**
Date	**5th March 2019**

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)