Trust Policy

Plymouth Hospitals NHS
NHS Trust

Internet Use Policy

Date	Version
December 2015	**5**

Purpose

This policy outlines the acceptable use of the internet provided by Plymouth Hospitals NHS Trust.

Who should read this document?

All staff that have access to the internet should read this document.

Key messages

This document will outline acceptable use of the internet when accessed using Trust devices. It will also signpost staff to other policies that may be of reference.

Accountabilities

Production	Information Governance Support Manager HR Business Partner Operational Support Manager (IM&T)
Review and approval	Policy Sub Group of Joint Staff Negotiating Committee
Ratification	Director of IM&T (CIO)
Dissemination	Operational Support Manager (IM&T)
Compliance	Operational Support Manager (IM&T)

Links to other policies and procedures

Staff Social Media Policy
Performance and Conduct Policy

Version History

V1	January 2005	Initial Document
V2	August 2007	Updated
V3	January 2009	Updated
V4.1	March 2013	Reviewed and updated
V4.2	February 2014	Minor amendment to job titles
V5	October 2015	Updated reflecting changes in monitoring

Last Approval	Due for Review
December 2015	December 2020

The Trust is committed to creating a fully inclusive and accessible service. By making equality and diversity an integral part of the business, it will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender

reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

As agreed with the Equality and Diversity Team, this policy does not require an Equality Impact Assessment.

1 Introduction

Internet access is provided for work related purposes, as access to many services is now provided over the internet. However, the Trust allows limited personal access.

2 Purpose, including legal or regulatory background

This policy defines what is deemed acceptable use and is relevant to all authorised users who have access to the internet through the computers owned or managed by Plymouth Hospitals NHS Trust.

The Acts of Parliament below are relevant to this policy:

- Computer Misuse Act 1990
- Copyright, Designs and Patents Act
- Regulation of Investigatory Powers Act 2000

3 Definitions

Offensive Material

Offensive material is defined by the NHS Equal Opportunity and Harassment Policy and includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive.

Download/Upload

This is the process in which data is sent to a computer. Whenever information is received from the internet, it is being downloaded to the computer. The opposite of this process is called uploading.

N3

This is the name of the network supplied to the NHS.

Registration Authority Process

Management of registration and access control to ensure that individuals who need to access the network have had their identity checked and that appropriate access is assigned.

Executable Programmes

Many computer files are executable programmes, ie they actually do something, they contain computer codes which might simply change the colour of your screen or might allow you to enter data into a form or at worst, destroy the contents of your computer hard disk.

Common executable files can be identified by their file ending, such as BAS, EXE, COM etc.

4 Duties

Plymouth ICT Services

Plymouth ICT Services are responsible for maintaining a safe and secure computing environment in the Trust. This includes monitoring of any access to the network to establish breaches of the Information Security Policy.

Plymouth ICT Service Desk

The ICT Service Desk will log and run requests for reports to support enforcement of this policy where non permissible access is suspected.

Human Resources Department

The Human Resources department take forward issues, in conjunction with managers that have been identified, in line with the Performance and Conduct Policy.

All Managers

Managers within the Trust are responsible for ensuring that the policy and its supporting standards are built into local processes and that there is ongoing compliance.

All Staff

All staff, whether permanent, temporary or contracted and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5 Authorised Users

Any person who wishes to access the internet must apply to become an authorised network user. This is granted on request of the user and authorised by a sponsor using the Registration Authority (RA) process.

All users must read the terms and observe the conditions of the RA01.

Access to the internet will only be through the N3 firewall connection.

No user is permitted to have a networked PC connecting to the internet or other network through a modem whilst logged on or connected to the Plymouth Hospitals NHS Trust network.

6 Permissible Access

Access to the internet is for work related purposes, i.e. for NHS work or for professional development and training.

Personal Use

Reasonable personal use is permitted for authorised users on the basis that this does not interfere with the performance of their duties, or impact on the network.

Personal access to the internet should be limited to outside of normal working times, i.e., during official breaks or before and after normal working times, unless authorised by the user's Line Manager. The Line Manager should ensure that all staff is aware what usage is deemed acceptable in their areas.

Authorised users must act in accordance with their manager's local instruction in conjunction with the ICT and HR departments.

7 Non Permissible Access

Offensive Material

Users are not permitted to access, display or download from internet sites that hold offensive material. Doing so is considered a serious breach and may result in disciplinary action in line with the Performance and Conduct Policy and potential prosecution.

Other than instances which demand criminal prosecution, the final arbiter on what is or is not offensive material, or what is or is not permissible access to the internet will be decided by the Line Manager in conjunction with the Human Resources department.

It is not permissible for a user to use a proxy website to try and hide their identity from monitoring.

Users who have innocently accessed a website that contains offensive material which has not been filtered should immediately log off and report this to their Line Manager and the ICT Service Desk by emailing plymouthictservicedesk@nhs.net. Failure to do so could result in disciplinary action.

Excessive Use

If it is suspected that there may be excessive use of the internet, the Line Manager together with the Human Resources department will undertake an investigation with reports provided by the Plymouth ICT Service Desk.

8 Download/Upload of Files

It is not permitted to download/upload executable files (files which are in themselves executable programmes) without the permission of Plymouth ICT Services.

All file downloads must be virus checked by the device.

File downloads must be done in accordance with the Copyright, Designs and Patents Act.

It is a breach of security to download files which disable the network or which have the purpose of compromising the integrity and security of the network and file servers. In

addition, to intentionally introduce files which cause computer problems could be prosecutable under the Computer Misuse Act 1990 and staff may be subject to disciplinary action under the Performance and Conduct Policy.

9 Use of Personal Information and the Trust Name

If a user joins a chat group or social network, that user is expected to conduct themselves in an honest and professional manner. The user is responsible for what they write and must be courteous and inoffensive.

Unless the user is authorised to do so, they are not permitted to write or present views on behalf of the Trust. This means that users cannot join a social network or chat group in the name of an NHS establishment or department, nor can they design a private website from their home PC and publish it under the name of an NHS establishment or department.

Staff must not publish any patient identifiable information without explicit consent on the internet.

10 Internet Filtering

The Trust employs the use of Fortigate to provide an internet filtering solution. This involves proactive blocking of websites which fall into certain categories.

Categories that have been blocked include (but are not limited to)

- Adult Materials
- Child Abuse
- Gambling
- Hacking
- Extremist Groups
- Illegal or Unethical
- Lingerie and Swimsuit
- Nudity and Risqué
- Phishing
- Plagiarism
- Pornography
- Proxy Avoidance
- Racism and Hate
- Sports Hunting and War Games
- Spyware and Malware
- Tasteless
- Tobacco
- Weapons
- Violence

11 Internet Monitoring

The Trust is responsible for establishing policy enforcement and will provide individual monitoring reports to Line Managers upon request.

12 Password Security

Each user is responsible for maintaining the security of their individual login and password. Users must not share their username or password with anyone. If inappropriate internet access is recorded under a user's login, the burden of proof will be with that user to show that they are not responsible for the breach.

13 Overall Responsibility for the Document

The Operational Support Manager (IM&T) has overall responsibility for this document.

14 Consultation and Ratification

The design and process of review and revision of this policy will comply with "The Development and Management of Trust Wide Documents".

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be approved by the Policy Sub Group of Joint Staff Negotiating Committee and ratified by the Director of IM&T (CIO).

Non-significant amendments to this document may be made, under delegated authority from the Operational Support Manager (IM&T), by the nominated author. These must be ratified by the Director of IM&T (CIO) and should be reported, retrospectively, to the approving committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

15 Dissemination and Implementation

Following approval and ratification, this policy will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with "The Development and Management of Trust Wide Documents".

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the named Executive Director and for

working with the Trust's training function, if required, to arrange for the required training to be delivered.

16 Monitoring Compliance and Effectiveness

The Trust monitors internet activity using Fortianalyser software to ensure compliance with this policy.

The Plymouth ICT Service Desk will respond to requests from Line Managers for staff usage reports. These will be provided on receipt of an email request and Line Manager/HR confirmation.

Dissemination Plan | Appendix 1

Core Information	
Document Title	Internet Use Policy
Date Finalised	December 2015
Dissemination Lead	Information Governance Support Manager
Previous Documents	
Previous document in use?	Yes
Action to retrieve old copies.	To be removed by Document Controller

Dissemination Plan

Recipient(s)	When	How	Responsibility	Progress update
All staff	December 2015	Vital Signs	Document Control	

Review and Approval Checklist | Appendix 2

Review		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
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
Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes
	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes