Notice:

Plymouth Community Healthcare Community Interest Company adopted all Provider policies from NHS Plymouth when it became a new organisation on 1 October 2011.

Please note that policies will be reviewed to reflect the new organisation in line with the reader information sheet, or sooner where this is possible.

NHS Plymouth

Internet Acceptable Use Policy

Version No 1.3

Notice to staff using a paper copy of this guidance

The policies and procedures page of Healthnet holds the most recent version of this guidance. Staff must ensure they are using the most recent guidance.

Author: **Information Governance Manager (PHT) adapted for NHS Plymouth by Information Governance Lead**

Access ID Number: **PTPCT G 290**

Reader Information and Asset Registration

Title	Internet Acceptable Use Policy.
Information Asset Register Number	PTPCT G 290
Rights of Access	Public
Type of Formal Paper	Policy
Category	Workforce
Format	Microsoft Word 2003 and PDF
Language	English
Subject	Information Security
Document Purpose and Description	Advise all Staff on responsibilities of internet usage
Author(s)/Editor(s) titles	Information Security Manager (PICTS), Business Development Manager & Information Governance Lead (NHS Plymouth)
Ratification Date and Group	November 2010
Publication Date	24/06/2011
Review Date and Frequency of Review	24/06/2013
Disposal Date	The Freedom of Information Office will retain a signed copy for the archive in accordance with the Retention and Disposal Schedule; all previous copies will be destroyed.
Job Title of Person Responsible for Review	Information Security Manager (PICTS), Business Development Manager & Information Governance Lead (NHS Plymouth)
Target Audience	All staff
Circulation List	Electronic: Via Healthnet Via NHS Plymouth website (subject to Freedom of information exemptions) Written: Upon request to the Policy Ratification Secretary on 01752 435104 or The Freedom of Information Manager on 01752 435112. Please note this document can be made available in other formats if required, please contact the Communications team on (01752) 435001. Please note if this document is needed in other formats or languages please ask the document author to arrange this as per the PCT's Quick Guide number 13.
Consultation Process	PHNT, IT Security Officer, Business Development Manager & Information Governance Lead, Information Strategy & governance Committee, Ratification Committee, JCCN
Impact Assessment	Yes

References/Source	The Computer Misuse Act 1990 The Copyright, Designs and Patents Act 1988 The Human Rights Act 1998 The Regulation of Investigatory Powers Act 2000
Supersedes Document	PHNT's Internet Acceptable use policy. V. 3.
Author Contact Details	**By post** NHS Plymouth Plymouth Primary Care Trust Building One Brest Road Derriford Plymouth PL6 5QZ **Telephone/fax** T: 01752 315315 F: 01752 315321 **Email** **ask@plymouth.nhs.uk**
Publisher: (for externally produced information)	

Document Review History

Version No.	Type of Change	Date	Originator of Change	Description of Change
1.1	New document	January 2010	Business Development Manager & IG Lead	Put into NHS Plymouth format from PHNT.
1.2	Updated	November 2010	Business Development Manager & IG lead	Changes made following ratification committee
1.3	Minor change	June 2011	Business Development Manager & IG Lead	Minor changes, Social networking information

Internet Acceptable Use Policy

This Policy is a Trust Wide Policy for the Acceptable Use of the Internet.

1. Rationale

Internet Access is provided primarily for professional related purposes, as access to many professional services are now provided over the Internet to distant computers and servers, the connection supplied by the NHS also allows direct access to the World Wide Web (Internet) and the Trust feels that limited personal access is permissible.

This Policy is set to define what is deemed acceptable use.

2. Applicable to

All authorised users who many or may not be employed by the NHS Plymouth, but who have authorised access to the Internet through the computers owned or managed by NHS Plymouth. This policy can also be applied to portable devices.

3. 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 process.

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

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 information communication technology service (PiCTS) network.

4. Permissible Access

Access to the Internet is primarily for professional related purposes. That is for NHS work or for professional development and training. Reasonable personal use is permitted for authorised users on the basis that this does not interfere with the performance of their duties, or the network.

Personal access to the Internet should be limited to outside of normal working times, ie, during official breaks or before and after normal working times, unless authorised by the user's Line Manager. The Line Manager, in conjunction with workforce development and information security will give guidance. Authorised users must act in accordance with their manager's local guidance/instruction in conjunction with information security and workforce development, who have the final decision on deciding what constitutes excessive use.

5. Non Permissible Access

No one is permitted to access, display or download from Internet sites that hold offensive material. Doing so is considered a serious breach of NHS Plymouth security and may result in dismissal/access to place of work being removed and/or prosecution. 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 and includes Internet and email. Other than instances, which demand criminal prosecutions, 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 information security and workforce development.

It is not permissible to use Internet radio or streaming media, eg live video, without the permission of the Information Security Team, as this has a serious impact on the bandwidth available to network users and has an impact on clinical applications.

Certain sites, which include Facebook, Bebo, YouTube and EBay are not permitted due to the high bandwidth they take up. If you need access to these sites for work purposes email information.security@phnt.swest.nhs.uk and clear with your line manager.

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 such a site that has not been filtered will log off immediately and report this to their Line Manager and the Information Security Team by email to information.security@phnt.swest.nhs.uk. Failure to do so could result in disciplinary action.

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 a breach of security 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.

5. 1. Download/Uploading of Files

It is not permissible to download/upload executable files (files which are in themselves, executable programmes) without the permission of the Information Security Team. These file types include, .exe. .com, .jap, .bas, .scr etc.

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 additions to intentionally introduce files which cause computer problems could be prosecutable under the Computer Misuse Act 1990 and you may be subject to Trust Disciplinary procedures.

5.2 Your Name and the Use of the Trust Name

If a user joins a chat group or news group, 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. Think twice before writing an angry email or contribution on a newsgroup. Unless the user is currently 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 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.

5.3 Use of Social Networking Sites

There are a vast number of social networking sites for both socialising and professional discussion. NHS Plymouth staff have a personal responsibility both in and out of the workplace whilst using social networking sites to maintain patient and staff confidentiality and professional standards at all times. Unauthorised disclosure of business information could be a potential confidentiality breach. Inappropriate photographs, comments or descriptions of your personal activities could bring both you and NHS Plymouth into disrepute and could be considered a disciplinary matter.

Staff:

- Should not reveal confidential information about our patients, staff, or NHS Plymouth
- Should not engage in activities on the Internet which might bring NHS Plymouth into disrepute.
- Should not use the Internet in any way to attack or abuse colleagues.
- Should not post photographs of the workplace or colleagues or patients
- Staff should not post information when they have been asked not to. They should also remove information about a colleague if that colleague asks them to do so.

6. Monitoring Access

PiCTS are responsible for establishing policy enforcement and monitoring of any access to the NHS Plymouth network to establish breaches of the IT Security Policy. This encompasses all network access and includes Internet access and

email usage. The PiCTS Head of Technology is responsible for ensuring that suitable audit tools are in use which enforce policy and monitor network usage and log by username and password the sites accessed, the time of day the sites were accessed and for how long and if a file transfer took place. This information must be made available to NHS Security Managers of Connecting for Health and/or the NHS Counter Fraud Team on request.

7. Responsibilities of the IT Services Department

7.1. NHS Code of Connection

The staff within PiCTS act as the delegated agents of the Chief Executive are responsible for maintaining a safe and secure computing environment in the Trust. More specifically they are responsible for ensuring that the NHS Plymouth conforms to the NHS Statement of Compliance and have fully implemented the NHS Security and Access Policy.

7.2. Excessive Use

If monitoring software identifies that there is excessive use of the Internet, the PiCTS infrastructure team will notify the Information Security Team who will raise the issue with the Line Manager of the individual.

7.3. Accessing Offensive Sites

If policy enforcement and monitoring software shows that a member of staff has been accessing a site identified as offensive, the Information Security Team must be immediately informed. It is the responsibility of the Information Security Team to inform the individual's Line Manager and/or the appropriate workforce development Officer and a Connecting for Health Security Manager (if a prosecution is possible) of the security breach. A full investigation will be undertaken which may result in disciplinary action being taken. When a breach is identified, the access of the person(s) NT account may be suspended pending investigation.

7.4. Dormant Accounts

If access is given to the Internet and is not used for at least a six month period, the account may be disabled. To re-enable the account the user must re-apply through the normal process.

8. Glossary

Bandwidth

Bandwidth refers to how much data you can send through a network or modem connection. It is usually measured in bits per second, or "bps". You can think of bandwidth as a highway with cars travelling on it. The highway is the network connection and the cars are the data. The wider the highway, the more cars can get to their destinations faster. The same principle applies to computer data – the more bandwidth, the more information that can be transferred within a given amount of time. Also the more users, the less bandwidth available so data transfer becomes slower.

Chat Room

A virtual room on the Internet where you can "chat" to people using the keyboard about any subject – although there are many specialised chat room dealing with specific issues.

Download/Upload

This is the process in which data is sent to your computer. Whenever you receive information from the Internet, you are downloading it to your computer. For example, you might have to download an upgrade for your computer's operating system in order to play a new game (especially if you're using Windows). Or you might download a demo version of a programme you are thinking about buying from the software company's website. The opposite of this process – sending information to another computer is called uploading.

Executable Files

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. Programmes like Explorer and Word are executable files and also the MYDOOM virus is an executable file which will destroy data.

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

N3

This is the name of the network supplied to the NHS and our entire Internet and remote clinical systems use this network to transfer information.

Virus

Like a biological virus, a computer virus is something you don't want to get. Computer viruses are small programmes or scripts that can that can negatively affect the health of your computer. These malicious little programmes can create files, move files, erase files, consume your computer's memory and cause your computer not to function correctly. Some viruses can duplicate themselves, attached themselves to programmes and travel across networks. In fact, opening an infected email attachment is the most common why to get a virus.

For more information visit: http://www.sharpened.net/glossary/main.php

9. Process to Monitor Compliance and Effectiveness if this Policy.

Compliance with this policy will be monitored by quarterly audits of access to the Internet by the Information Security Team.

Breaches of this policy are to be recorded as incidents using the Trust Incident Reporting Process.

All policies are required to be signed by the Lead Director or Assistant Director. (The policy will not be accepted onto Healthnet until signature is received.)

The proof of signature for all policies is stored in the office with the Freedom of Information Officer.

The Lead Director, Assistant Director or Head of Service approves this document and any attached appendices.

Signed: ……

Date: ……