Western Health
and Social Care Trust

INTERNET POLICY

September 2014

Version 3.0

Policy Title	INTERNET POLICY
Policy Reference Number	CORP09/007
Original Implementation Date	September 2009
Revised Date	September 2014
Approved Date	November 2014
Review Date	November 2016
Responsible Officer	FERGAL DUREY, AD for ICT and Telecommunications

Table of Contents

1. Background and Purpose

The Internet is a significant business, information and communication tool for the Western Health and Social Care Trust (WHSCT) and staff need to be aware of their personal responsibilities with regards to its use and the potential consequences resulting from misuse. Failure to comply with this policy may lead to disciplinary action.

The Trust employs Internet technologies to provide access to the information resources that will assist employees to carry out their duties more efficiently and effectively. The provision of these services requires the commitment of considerable organisational resources in respect of infrastructure and support. Therefore it is necessary that the Trust take steps to safeguard the provision of these services and, where appropriate, any information or data stored.

The purpose of this policy is to ensure proper and appropriate use of the Internet by making staff aware of the organisation's definition on acceptable and unacceptable use.

The measures outlined in this policy will not be effective without the cooperation of all Western Trust staff. The cooperation of all such staff, and acceptance of this policy, is therefore a prerequisite to approval for Internet access.

2. Guidelines for staff

The set-up and management of all user accounts is governed in accordance with guidelines and principles found in the *WHSCT Management of User Accounts and Password Policy*.

Only authorised equipment belonging to the Trust may be used for access to the Internet.

Staff <u>must</u> ensure that they use Internet services lawfully at all times

The Trust reserves the right to review the use of the Internet as it deems appropriate.

To protect both the organisation and the employee the following list is illustrative (indicative) of the type of activity that the Trust considers to be 'Unacceptable Use'.

No information published unless approved by the Trust Communications Department.

Publishing Trust user account or password details on any Web site *outside* the HSCNI network.

The transmission of Trust user account and/or password details via social network sites (e.g. Bebo, Facebook, Twitter,etc). The transmission of Trust user account and/or password details to e-mail systems outside the HSCNI network (e.g. Hotmail, Gmail etc)

The transmission of material that is defamatory, illegal, offensive or may cause, or lead to, harassment.

- Violation of copyright (including intellectual). For example, downloading, installation and / or onward distribution of 'pirated' software or media.

- Successful or unsuccessful attempts to gain unauthorised access to systems, sites or information sources – commonly referred to as 'hacking'.

- Using any method to disguise Internet activity. This includes the use of proxy-avoidance technologies and / or changing the configuration of Internet browser software without prior consent or authorisation.

Personal use

Internet access in a Western Trust facility is intended to support the organisation's legitimate business requirements. However, occasional and reasonable use of the Internet for personal purposes is regarded as acceptable provided that:
- Must be at the discretion of your line manager
- Must be within staff's own time and not interfere with other staff carrying out their work duties.
- The user must not create any unauthorised contractual liability on the part of the Trust.
- The Trust will not accept any liability for financial loss while using Trust systems for personal transactions.
- The Trust reserves the right to monitor Internet activity where it suspects private use is inappropriate or excessive.
- Users might be personally liable to prosecution, and open to claims for damages, if their actions are found to be in breach of the law.
- Access is not used for private business or other commercial purposes

Note: Disclosing personal information on the Internet increases the risk of identity theft, for more information staff are encouraged to follow government guidance at www.identitytheft.org.uk.

Webmail (E-mail on the Internet)

- Only access to *doctors.net.uk and approved web mail services* will be allowed via a web browser
  Further exceptions will be at the discretion of the AD for ICT and Telecommunications.

3. Countermeasures

This policy should be seen as one of a number of countermeasures put in place to protect the organisation and its employees from such things as inadvertent exposure to illicit material, malicious software etc, and also the possibility of legal action as a direct result of Internet abuse or misuse. Additional protection is provided by the following:-

- **Limited Access**
  Access is limited to certain sites and categories. Those sites and categories that have been restricted are too numerous to mention and are kept under constant review. Where access is required for business purposes restrictions may be relaxed with express approval from the relevant director responsible for the service in conjunction with the AD for ICT and Telecommunications. .

- **Prohibited**
  Certain material such as video and audio streaming, audio and software downloads is prohibited. The Trust will endeavour to provide access to this material if required for business use where it can be ensured that it will not have a detrimental effect on the service and where the network infrastructure permits.

- **Monitoring**
  i)   The Trust reserves the right to monitor the use of the Internet.
  ii)   Suspected cases of abuse of the Internet or breaches in policy will be rigorously investigated within HR guidelines and in conjunction with HR staff.

- **Removal**
  i)   Internet access may be withdrawn at any time as a result of, or pending the outcome of, investigations into suspected abuse or misuse
  ii)   User accounts will be terminated for staff who leave the organisation
  iii) Dormant user accounts not otherwise accessed on a regular basis, will be deemed suitable for removal. Special leave or periods of extended absence will be taken into consideration.

4. Transfer of Trust information via the internet

Uploading, where appropriate, to the Internet is only permitted where approval has been provided. The following points must be borne in mind;
  i)   an authorised Data Access Agreement **must** to be in place before uploading of any business sensitive or Patient/Client information.
  ii) Patient/client confidentiality **must** be maintained. Data must be anonymised and encryption tools used before uploading.

Further information can be obtained from the Information governance policy on the Transfer of Data

5. Additional Resources

This policy should be read in conjunction with other policies relating to effective and appropriate use of ICT services, including:
1) WHSCT E-mail Policy
2) WHSCT Management of User Accounts and Password Policy.
3) WHSCT Server, Desktop and Portable Security Policy
4) WHSCT Malicious Software Policy
5) WHSCT Social Media
6) BSO ICT policies
7) WHSCT Protocol for the Electronic Transmission of Confidential Information by Fax and Email

6. Training

The Trust is committed to staff development and seeks to consistently improve development standards and opportunities for staff in line with organisational objectives and policies and procedures. Should you or your staff require support in the effective use of ICT please contact the ICT Training Team via the ICT Service Desk.

7. Equality & Human Right's Statement

The Western Health & Social Care Trust's Equality and Human Right's statutory obligations have been considered during the development of this policy.

8. Further Information

For further information in relation to this policy please refer to:-

The ICT User Forum on the ICT service desk portal available on the Trust intranet link below.

(http://wta-eservicedesk/portal/)

.