NHS Wales
All Wales Internet Use Policy

Issue Date: 7 January 2016
Review Date: January 2018

1 DOCUMENT HISTORY

1.1 Revision History

Date	Version	Author	Revision Summary
7/9/15	V0.87	Andrew Fletcher / Darren Lloyd, NWIS (on behalf of the Internet and Email policy sub group)	Final Draft
29/9/15	V0.88	Andrew Fletcher / Darren Lloyd, NWIS (on behalf of the Information Governance Management and Advisory Group)	Minor amendment (as a condition of approval)
1/12/15	V0.89	Andrew Fletcher / Darren Lloyd, NWIS (on behalf of the Information Governance Management and Advisory Group)	Minor amendments (as a result of Equality Impact Assessment)

1.2 Reviewers

This document requires the following reviews:

Date	Version	Name	Position
12/08/15	V0.86	Internet and Email policy sub group	Representation from all NHS Wales Information Governance, Information Security, Communications and Human Resources
29/09/15	V0.87	Information Governance Management and Advisory Group	All Wales Information Governance Leads
23/10/15	V0.88	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)
1/12/15	V0.89	Equality Impact Assessment Panel	Independent equality impact assessment
3/12/15	V1	Welsh Partnership Forum	

Scope

This policy applies to all users of the NHS Wales IT network including staff; students; trainees; secondees; volunteers and contracted third parties.

The policy describes the principles which must be adhered to by all in the use of the World Wide Web (or Internet), the NHS Wales Network (which is defined as a corporate Intranet) and other affiliated sites.

The terms “Internet access” or “Internet use” encompass any use of any resources of the World Wide Web including social media / social networking, browsing, streaming, downloading, uploading, posting, “blogging”, “tweeting” chat and email. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

This policy applies to all staff that make use of the NHS network infrastructure and / or NHS equipment to access internet services regardless of the location from which they accessed and the type of equipment that is used including corporate equipment, third party and personal devices.

Position Statement

NHS Wales trusts its workforce in using NHS Wales equipment.

Internet access is provided to staff to assist them in the performance of their duties and the provision of these facilities represents a major commitment on the part of NHS Wales in terms of investment and resources.

The NHS Wales workforce should become competent in using internet services to the level required for their role in order to be more efficient and effective in their day-to-day activities.

NHS Wales will support its workforce in understanding how to safely use internet services and it is important that users understand the legal professional and ethical obligations that apply to its use. If used correctly, the internet can increase efficiency and safety within patient care.

The effectiveness of this policy will be assessed to provide assurance that risks to information and likelihood and impact of information security incidents are being reduced.

Conditions & Restrictions

To avoid inadvertent breaches of this policy, inappropriate content will be blocked by default where possible. In general, inappropriate material must not be accessed. For the avoidance of doubt, subject matter considered inappropriate to access is detailed in appendix A.

Some sites may be blocked by default due to their general impact on network resources and access to these for work purposes can be requested by contacting the Local IT Service Desk

In general, regardless of where accessed (for example - at work or at home), NHS Wales employees must not, at any time, participate in any online activity or create or transmit or store material that is likely to bring the organisation into disrepute or incur liability on the part of NHS Wales.

Business Sensitive Information or Personal Identifiable Information (PII) including photographs and video recordings of patients, members of the public, or other members of staff taken on NHS Wales premises must not be uploaded to online storage, media sharing sites, social media, blogs, chat rooms or similar without both the authorisation of a head of service and the consent of the individual who is the subject of that recording. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

It is each user's responsibility to ensure that their Internet facilities are used appropriately. Managers are reminded that, as an NHS Wales resource, the Internet is in many ways similar to the telephone systems and should be managed accordingly.

Personal Use

NHS Wales organisations allow staff reasonable personal use of internet services providing this is within the bounds of the law and decency and compliance with policy.

Personal use should be incidental or reasonable (as a threshold NHS Wales defines a maximum of thirty minutes in one shift / working day as reasonable) and before or after normal working hours, or during agreed break times. These limitations are also necessary due to network demands and therefore local restrictions may apply dependent on the duration of access and the capacity of resources available. In addition to this users must not download large files as these may have a negative impact on network resources including bandwidth and storage. Staff should be aware that downloading from the internet may also expose the NHS Wales network to viruses and malicious code.

Where local organisations have provided patients and staff with cloud internet services (for example – free public Wi-Fi), employees are encouraged to use these facilities by default on personally-owned devices instead of using NHS equipment. Local agreements will be in place for the use of and availability of these facilities.

Staff who use NHS equipment outside NHS Wales premises (for example – in a home environment) are permitted to connect to the Internet. Use of the Internet under these circumstances must be through the secure VPN connection provided by the NHS Wales organisation. Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy.

All personal use of the Internet is carried out at the user's own risk. The NHS Wales does not accept responsibility or liability for any loss caused by or liability arising from personal use of the Internet. The HB's Internet access facility must not be used to run or support any kind of paid or unpaid personal business venture outside work, whether or not it is conducted in a user's own time or otherwise.

At no time should access to the Internet be used by any individual for personal financial gain (E.g. selling on eBay or any other auction sites).

Monitoring

NHS Wales accept that reasonable personal use will occur and staff must be aware that NHS Wales reserves the right to monitor the use of the internet by any employee and may come under scrutiny. This will mean that computers which are used for personal reasons will potentially be monitored.

NHS Wales organisations respect the privacy of its employees and does not want to interfere in their personal lives but the monitoring of a secure network and checking on the use of time is a legitimate business interest. Regardless if the equipment is personal or NHS property if it utilises NHS internet resources it will be subject to network monitoring.

NHS Wales uses software to automatically and continually record the amount of time spent by staff accessing the Internet and the type of websites visited by staff. Attempts to access any prohibited websites which are blocked is also recorded.

Staff should be reassured that NHS Wales organisations take a considered approach to monitoring individual usage of the Internet, however it reserves the right to adopt different monitoring patterns as required. In the main monitoring is normally conducted on the basis that such usage is suspected to be in breach of either a NHS Wales policy or legislation. Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

It is recognised that minor breaches may sometimes inadvertently occur and managers are therefore encouraged to speak to staff of their concerns should any minor issues arise. If serious breaches are detected following discussions with staff and where continual repeated misuse is detected, an investigation will take place. Where this or another policy is found to have been breached, disciplinary action may be taken.

All audits and logs will be retained in line with NHS Wales retention and disposal schedules and Department for Health and Social Care Guidance. Additional audits or monitoring reports can be requested by line managers and may be activated in the system with the agreement of the relevant Head of Service.

Concerns about possible fraud and or corruption carried out using the NHS Wales internet functionality should be reported to the counter fraud team.

Review and revision arrangements

This document is issued and maintained by the NHS Wales Informatics Service (NWIS) on behalf of all NHS Wales organisations.

This policy will be reviewed as per the review date on the policy front sheet. However it will be reviewed where it will be affected by major internal or external changes such as:

- Legislation;
- Practice change or change in system/technology; or
- Changing methodology.

Training

Training relating to this policy must take place during the induction programme for new staff or as part of refresher training.

Appendix A

Inappropriate use

For the avoidance of doubt, NHS Wales organisations will generally consider any of the following inappropriate use:

- Excessive personal use;
- Allowing access to NHS Wales internet services by anyone not authorised to access the services, such as by a friend or family member;
- Communicating or disclosing confidential or sensitive information via the internet without authorisation or without the appropriate security measures being in place;
- Communicating any information which may cause offensive or embarrassment; including that which can be reasonably deemed to be defamatory, abusive, hateful, racist, sexist, homophobic, transphobic, discriminatory, indecent, obscene, pornographic, unlawful or involves violence, bullying or harassment.
- Communicating or disclosing material that is intended to (or in the organisation's view, is likely to) distress, annoy or intimidate another person or is contrary to the organisation's Dignity at Work Policy.
- Downloading, uploading, transmitting, viewing, publishing, storing or distributing defamatory material or intentionally publishing false information about NHS Wales or its staff, clients or patients.
- Knowingly access, or attempted access to, internet that contain obscene, hateful, pornographic, violent, terrorist, racist, sexist, homophobic, transphobic or otherwise illegal material. This will include such pages on social media sites.
- Knowingly and without authority view, upload, or download material that may bring NHS Wales into disrepute; or material that could cause offence to others.
- Sending or saving information or images which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist, sexist, homophobic and transphobic or illegal material.
- Downloading or installing or distributing unlicensed or illegal software.
- Downloading software without authorisation or changing the configuration of existing software using the Internet without the appropriate permissions.
- Breaching copyright or Intellectual Property Rights (IPR).
- 'Hacking' into others accounts or unauthorised areas.
- Deliberately attempting to circumvent security systems protecting the integrity of the NHS Wales network.
- Any purpose that denies service to other users (for example, deliberate or reckless overloading of access links or switching equipment).
- Intentionally introducing malicious software such as Viruses, Worms, and Trojans into the NHS Wales network.
- To access sites with the intention of making a personal gain (for example - running a business).
- Access to Internet based e-mail providers including services such as Hotmail, Freeserve, Tiscali

etc is prohibited for reasons of security with the exception of:

  - Access to email services provided by a recognised professional body or a trade union recognised by the employer;
  - The Doctors.net email service;
  - Any UK university hosted e-mail account (accounts ending in .ac.uk);
  - Any email account hosted by a body which the employee contributes to in conjunction with their NHS role, such as a local authority or tertiary organisation.

- Altering any of the system settings on a NHS Wales owned PC or try to change the access server in an attempt to avoid the restriction imposed by the filtering software. This will be deemed as a breach of this policy and will be dealt with under the All Wales Disciplinary Policy.