GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	Reference Number: PHW84 Version Number: 1.0 Date of next review: May 2027

INTERNET ACCEPTABLE USE POLICY

Policy Statement

This policy provides direction to Public Health Wales staff on appropriate use of internet facilities to deliver our services. The policy also sets out the responsibilities of all users when using the internet.

This policy must be read in conjunction with relevant organisational procedures.

Policy Commitment

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 be competent in using internet services to the level required for their role in order to be efficient and effective in their day-to-day activities. Public Health 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 business efficiency and service user safety.

Supporting Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

All Wales Information Governance Policy
All Wales Social Media Policy

Scope

This policy applies to the Public Health Wales workforce including staff, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of Public Health Wales. 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.

Equality and Health Impact Assessment	An Equality, Welsh Language and Health Impact Assessment has been completed and can be viewed on the policy webpages.
Approved by	Audit and Corporate Governance Committee
Approval Date	09/05/2024
Review Date	09/05/2027
Date of Publication:	08/07/2024
Group with authority to approve supporting procedures	Senior Leadership Team
Accountable Executive Director/Director	Iain Bell, Senior Information Risk Owner and National Director of Public Health Knowledge and Research
Author	John Lawson, Head of Information Governance

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Board Business Unit

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
0.1	15/01/2024			New Policy to replace withdrawn All Wales Policy
1.0	01/05/2024	09/05/2024	08/07/2024	

1. Introduction

The policy describes the principles which must be adhered to by all in the use of the 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 internet 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.

2. Roles and Responsibilities

The Chief Executive is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation and any associated legal requirements. Specific responsibilities will be delegated to the Senior Information Risk Owner, the Caldicott Guardian, the Data Protection Officer, and or an Executive Director as appropriate.

Managers are responsible for the implementation of this policy within their department/directorate. In addition, they must ensure that their staff are aware of this policy, understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training. Breaches of the policy must be reported via local incident reporting processes and dealt with in line with the All Wales Disciplinary Policy where appropriate.

All staff must understand that they are personally accountable for their use of the internet, both for official work purposes and for personal use as permitted within this policy.

Staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. Mandatory information governance training must be undertaken at least every two years. Breaches of this policy must be reported via local incident reporting processes.

3. Conditions and Restrictions

To avoid inadvertent breaches of this policy, inappropriate use will be blocked by default where possible. Inappropriate material must not be accessed. Exceptions may be authorised for certain staff where access to particular web pages are a requirement of the role.

Examples of subject matter considered inappropriate is detailed in appendix A.

Additionally, 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 Public Health Wales IT Service Desk.

Regardless of where accessed users must not 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 Public Health Wales.

Business Sensitive Information or Personal Data (which includes photographs and video recordings) of any patient, member of the public, or member of staff taken on NHS Wales premises must not be uploaded to any form of non-Public Health Wales approved 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 Data Subject of that recording. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

It is each staff member'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.

4. Personal use of the internet

Although Public Health Wales encourages staff to use personal devices (such as mobile phones or tablets) to access the internet for personal use, it does permit staff reasonable personal use of internet services through our own IT systems providing this is within the bounds of the law and decency and compliance with this policy.

Limitations on use are necessary due to network demands and the need to ensure that network resources are available for business purposes. Personal use therefore should be incidental and reasonable and should normally take place before or after normal working hours, or during authorised break times.

Staff must not stream or download large volumes of data (e.g. streaming audio or video, multimedia content, software packages) for personal purposes as these may have a negative impact on network resources.

Staff who use NHS equipment outside NHS Wales premises (e.g. working from home) are permitted to connect to the internet but any connection under these circumstances must be through the secure connection provided by the organisation (for example via Virtual Private Network, Multi Factor Authentication). 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. Public Health Wales does not accept responsibility or liability for any loss caused by or liability arising from personal use of the internet.

Internet access facilities 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. using eBay or any other auction sites).

5. Training and Awareness

Information governance is everyone's responsibility. Training is mandatory for NHS staff and must be completed at commencement of employment and at least every two years subsequently. Non NHS employees must have appropriate information governance training in line with the requirements of their role.

6. Monitoring and compliance

Public Health Wales trusts its workforce, respects the privacy of its staff and does not want to interfere in their personal lives but proportionate monitoring of work processes is a legitimate business interest.

Public Health Wales therefore reserves the right to monitor work processes including use of the internet to ensure the effectiveness of the service. This will mean that any personal activities that the employee practices in work may come under scrutiny.

Public Health 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, however it reserves the right to adopt such monitoring methods and patterns as may be deemed appropriate from time to time..

Managers are expected to speak to staff about their concerns should any minor issues arise. If breaches are detected an investigation may take place. Where this or another policy is found to have been breached, disciplinary procedures will be followed.

Managers must report any concerns about possible fraud and/or corruption to the NHS Wales counter fraud team.

7. Review

This policy will be reviewed every three years or more frequently where the contents are affected by major internal or external changes such as:

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

8. Equality Impact Assessment

This policy has been subject to an equality assessment.

Following assessment, this policy was not felt to be discriminatory or detrimental in any way with regard to the protected characteristics, the Welsh Language or carers.

Appendix A - Inappropriate use

The following are examples of what would be considered inappropriate use. This list is not exhaustive and staff must use personal judgement on what may or may not be appropriate. If in any doubt, the intended use must be avoided until proper authorisation has been obtained.

- Excessive use for personal purposes.

- Allowing access to Public Health Wales internet services by anyone not authorised to access the services, such as by a friend or family member.

- Knowingly or recklessly communicating or disclosing confidential or sensitive information via the internet without authorisation or without the appropriate security measures being in place.

- knowingly or recklessly and without proper authorisation or lawful purpose downloading,uploading, storing, saving, communicating, publishing or distributing any information or images which are unlawful, defamatory, maliciously false, offensive, abusive, obscene, hateful, pornographic, violent, terrorist, indecent or being discriminatory in relation to the protected characteristics or which may otherwise bring PHW or NHS Wales into disrepute

•• Knowingly or recklessly and without proper authorisation or lawful purpose accessing, or attempting to access internet sites that contain such material or otherwise illegal material. This will include such pages on social media sites.

- • 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).

- Altering any of the system settings on a Public Health Wales owned device or trying 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.