CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

NHS Wales
Internet Use Policy for
Primary Care Service Providers

Author: IG Support for Primary Care, DHCW
Approved by: Darren Lloyd,
Associate Director of Information Governance & Patient Safety, DHCW
Version: Final V2.0
Date: April 2022
Review date: April 2024

Ty Glan-yr-Afan
21 Heal Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD
21 Cowbridge Road East, Cardiff CF11 9AD
Ffon/Tel: 02920 500500
www.cymru.nhs.uk/gwybodeg
www.wales.nhs.uk/informatics

Document History

Revision History

Date	Version	Author	Revision Summary
19/11/2020	D0.1	Francesca Harries	Initial draft developed supplementary to the All Wales Internet Use Policy V2
20/11/2020	D0.2	Jeannette Short	Suggested updates
30/11/2020	D0.3	Francesca Harries	Further updates
01/12/2020	D0.4	Francesca Harries	Updates following review by Darren Lloyd
02/12/2020	D0.5	Francesca Harries	Updates in line with the All Wales Internet Use Policy V2.1
07/12/2020	V1.0	Francesca Harries	
13/09/2021	D1.1	Sarah Muirhead	Updated 'NWIS' to 'DHCW'
14/03/2022	D1.2	Jeannette Short	Review/Updates
25/03/2022	D1.3	Francesca Harries	Updates following review by Darren Lloyd
11/04/2022	V2.0	Francesca Harries	

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
01/12/2020	D0.3	Darren Lloyd	Head of Information Governance, DHCW
04/12/2020	D0.5	Darren Lloyd	Head of Information Governance, DHCW
14/03/2022	D1.2	Jeannette Short	Primary Care Support and IG Assurance Manager, DHCW
25/03/2022	D1.2	Darren Lloyd	Associate Director of Information Governance & Patient Safety, DHCW

Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name:	Francesca Harries
Role:	Information Governance Assurance Officer
Signature:	11/04/2022 X Francesca Harries Francesca Harries Information Governance Assurance Officer Signed by: Francesca Harries (Fr215649)

Approver's Name:	Darren Lloyd

Role:	Associate Director of Information Governance & Patient Safety
Signature:	11/04/2022 X  Darren Lloyd Associate Director of Information Governan... Signed by: Francesca Harries (Fr215649)

Contents

1. Introduction

This document is supplementary to the All Wales Internet Use Policy issued under the All Wales Information Governance Policy Framework and is maintained by Digital Health and Care Wales (DHCW) on behalf of all NHS Wales organisations.

2. Purpose

This policy provides assurance that the NHS Wales internet facilities are being used appropriately to assist in delivering services.

The policy also sets out the responsibilities of all users when using the internet. These responsibilities include, but are not restricted to, ensuring that:

- The confidentiality, integrity, availability and suitability of information and NHS Wales computer systems are maintained by ensuring use of internet services is governed appropriately;
- All individuals as referenced within the scope of this policy are aware of their obligations.

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

3. Scope

This policy applies to all staff (users) of Primary Care Service providers who benefit with access to NHS Wales Internet facilities via the NHS Wales network infrastructure.

The term 'staff' includes all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the Primary Care Service provider.

For the purpose of this policy 'Primary Care Service providers', referred to in this policy as 'the Organisation' will include General Medical Practices, Pharmacies, Dentists and Optometrists commissioned to provide primary care services on behalf of NHS Wales.

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.

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

4. Roles and Responsibilities

The Senior Responsible Person within the Organisation is responsible for ensuring the highest level of organisational commitment to this policy and the availability of resources to support its implementation and any associated legal requirements. Specific responsibilities may be delegated to the representative Data Protection Officer and other individuals who have responsibility for information governance within the organisation. See Appendix A for Glossary of Terms.

In addition, they must ensure that all staff are aware of this policy understand their responsibilities in complying with the requirements of this policy 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 Organisation's Disciplinary Policy where appropriate.

The workforce 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.

5. Policy

5.1. Policy Statement

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 workforce of the Organisation 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 and the Organisation will support the workforce in understanding how to safely use NHS Wales 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.

5.2. Conditions and Restrictions

To avoid inadvertent breaches of this policy, inappropriate content accessed through NHS Wales internet facilities 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. Subject matter considered inappropriate is detailed in Appendix B.

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 DHCW 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 NHS 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 or the primary Care Service Providers premises must not be uploaded to any form of non NHS approved online storage, media sharing sites, social media, blogs, chat rooms or similar, without both the authorisation of a Senior Responsible Person and the consent of the individual who is the Data Subject of that recording.

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 use of other forms of communications technology and should be managed accordingly.

5.3. Personal Use

NHS Wales and the Organisation 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 and reasonable. As a threshold, NHS Wales defines this as a maximum of thirty minutes in one calendar day 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 stream or download large volumes of data (e.g. streaming audio or video, multimedia content, software packages) as these may have a negative impact on network resources and have potential to impact NHS Wales systems and services.

Where the Organisation has provided patients and staff with access to public Wi-Fi services, 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 of the Organisations or NHS Wales premises (for example – in a home environment) are permitted to connect to the internet. Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy. Secure NHS Wales sites may require access via a secure connection provided by NHS Wales, for example, Virtual private Network (VPN) tokens or Multi Factor Authentication (MFA).

All personal use of the internet is carried out at the user's own risk. The Organisation and NHS Wales do 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).

6. Training and Awareness

Information governance is everyone's responsibility. Training is mandatory for all staff providing NHS services and must be completed at commencement of employment and at least every two years subsequently.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact their Senior Responsible Person as appropriate.

7. Monitoring and Compliance

NHS Wales and the Organisation trusts their workforce; however, they reserve the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that staff practice in work may come under scrutiny. NHS Wales and the Organisation respect the privacy of their staff and do not want to interfere in their personal lives however, monitoring of work processes is a legitimate business interest.

Where applicable to individual organisations delivering NHS Services, software may be used 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 may be blocked by other proprietary software supporting the appropriate use of the internet.

Staff should be reassured that NHS Wales and the Organisation take a considered approach to monitoring; however, they reserve the right to adopt different monitoring patterns as required. Monitoring is normally

conducted where it is suspected that there is a breach of either policy or legislation or when a manager has concerns around employee's performance, (e.g. excessive internet usage). Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

Managers are expected to speak to staff of 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.

Concerns about possible fraud and or corruption should be reported to the appropriate Counter Fraud Team.

In order for the Organisation to achieve good information governance practice, staff must be encouraged to recognise the importance of good governance and report any breaches to enable lessons learned. They must be provided with the necessary tools, support, knowledge and training to help them deliver their services in compliance with legislation. Ultimately a skilled workforce will have the confidence to challenge bad information governance practice and understand how to use information legally in the right place and at the right time. This should minimise the risk of incidents occurring or re-occurring.

8. Review

This policy will be reviewed one year after implementation and every two years thereafter 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.

9. 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 – Glossary of Terms

Term	Definition
Primary Care Service providers	General Medical Practices, Pharmacies, Dental Practices and Optometrists
Senior Responsible Person	**General Medical Practice –** Senior Partner, Caldicott Guardian, Data Protection Officer, Senior Information Risks Officer, Information Governance Lead, Practice Manager **Pharmacies –** Pharmacy Owner, Superintendent **Dental Practice** – Senior Partner, etc **Optometrists** – Senior Partner, etc
Staff	This is not an exhaustive list: all health professionals, partners, employees, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of the Primary Care Service provider.

Appendix B - Inappropriate use

For the avoidance of doubt, NHS Wales 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; Downloading or communicating any information or images which are unlawful, or could be regarded as defamatory, offensive, abusive, obscene, hateful, pornographic, violent, terrorist, indecent, being discriminatory in relation to the protected characteristics,; or using the email system to inflict bullying or harassment on any person;
- 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 accessing, or attempting to access internet sites that contain obscene, hateful, pornographic, violent, terrorist, racist 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 or the Organisation 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 or otherwise 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 Gmail, Hotmail, Yahoo 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;
    - 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 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 Organisation's Disciplinary Policy.

Annex 1: Equality Impact Assessment

Note: This EQIA has been taken from the original All Wales Internet Use Policy

Equality Impact Assessment (EQIA) Form		
Ref no: POL/IGMAG/Internet Use/v1		
Name of the policy, service, scheme or project:	Service Area	
NHS Wales Email Use Policy	Information Governance	
Preparation		
Aims and Brief Description	The policy is the product of the review of the All Wales Internet Use Policy.	
Which Director is responsible for this policy/service/scheme etc	All Wales policy developed in conjunction with Health Boards/Trusts	
Who is involved in undertaking the EQIA	Andrew Fletcher and EQIA Group	
Have you consulted with stakeholders in the development of this policy?	Yes. A sub group has developed this policy with a membership consisting of information governance leads and an OSSMB representative. IM&T leads and the Wales Partnership Forum have been consulted. The NHS Wales Information Governance Management and Advisory Group have approved the text of this Policy. The policy will be approved by the Wales Information Governance Board.	
Does the policy assist services or staff in meeting their most basic needs such as; Improved Health, fair recruitment etc	Yes. The policy will stand as a single internet use policy for NHS Wales. As per the original all-Wales Policy, it removes many of the restrictions which were in place in some organisations, while strengthening the governance framework. A key driver during the process was the need to recognise that organisations needed to trust their staff.	
Who and how many (if known) may be affected by the policy?	All users of the NHS Wales internet service within General Medical Practices, Pharmacies, Dentists and Optometrists who provide primary care services on behalf of NHS Wales	
What guidance have you used in the development of this service, policy etc?	The policy is based on good practice and legal obligations as set out by the Information Commissioners Office and in the legislation. The policy has also been constructed from existing agreed principles and the corporate knowledge of its stakeholders.	

Equality Duties

The Policy/service/project or scheme aims to meet the specific duties set out in equality legislation.	Protected Characteristics										
	Race	Sex/Gender	Disability	Sexual orientation	Religion and Belief	Age	Gender reassignment	Pregnancy and Maternity	Marriage & civil Partnerships	Welsh Language	Carers
To eliminate discrimination and harassment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote equality of opportunity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote good relations and positive attitudes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encourage participation in public life	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
In relation to disability only, should the policy / service / project or scheme take account of difference, even if involves treating some individuals more favourably?							✓				

Key	
✓	Yes
x	No
-	Neutral

Human Rights Based Approach – Issues of Dignity & Respect

The Human Rights Act contains 15 rights, all of which NHS organisations have a duty. The 7 rights that are relevant to healthcare are listed below.			
Consider is the policy/service/project or scheme relevant to:	**Yes**	**No**	**N/A**
Article 2: The Right to Life	X		
Article 3: the right not to be tortured or treated in a inhumane or degrading way	X		
Article 5: The right to liberty	X		
Article 6: the right to a fair trial	X		
Article 8: the right to respect for private and family life	X		
Article 9: Freedom of thought, conscience and religion	X		
Article 14: prohibition of discrimination	X		

Measuring the Impact

What operational impact does this **policy, service, scheme or project**, have with regard to the Protected Characteristics. Please cross reference with equality duties	
	Impact – operational & financial
Race	There is a consistent approach to IT policies across NHS Wales, this is an extension of the approach to put clear boundaries in place for staff, a revision of restrictions and identifying the need to respect and trust our staff. There is a clear statement around behaviours making it explicit that hateful and discriminatory language will not be accepted. There needs to be a wider understanding and context of trigger words. Dignity and respect of those using Internet policy as individuals and staff and clear instructions so staff know what is applicable to them.
Sex/gender	
Disability	
Sexual orientation	
Religion belief and non belief	
Age	
Gender reassignment	
Pregnancy and maternity	
Marriage and civil partnership	
Other areas	
Welsh language	
Carers	

Outcome report

Equality Impact Assessment: Recommendations

Please list below any recommendations for action that you plan to take as a result of this impact assessment

Recommendation		**Action Required**	**Lead Officer**	**Time-scale**	**Resource implications**	**Comments**
1	Communication of the changes	Make sure staff aware of the changes	AF	ASAP	Time	
2	Updated EQIA statement	Inclusion of reference to protected characteristics	AF	ASAP	Time	

Recommendation	**Likelihood**	**Impact**	**Risk Grading**
1	2	2	4
2	2	2	4

Risk Assessment based on above recommendations

Reputation and compromise position			Outcome
The policy is clear so that all staff aware of responsibilities and therefore reputation of organisation is preserved.			A clear understanding of the policy and responsibilities of staff in the use of IT in the workplace.
Training and dissemination of policy			
The policy is clear so that all staff aware of responsibilities and therefore reputation of organisation is preserved.			
Is the policy etc lawful?	**Yes** ☒	**No** ☐	**Review date**
Does the EQIA group support the policy be adopted?	**Yes** ☒	**No** ☐	**3 years**
Signed on behalf of NWIS Equal Impact Assessment Group	S Brooks	Lead Officer	
Date:	8 May 2018	Date: 8 May 2018	

	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Statutory duty	No or minimal impact or breach of guidance / statutory duty Potential for public concern Informal complaint Risk of claim remote	Breech of statutory legislation Formal complaint Local media coverage – short term reduction in public confidence Failure to meet internal standards Claims less than £10,000 Elements of public expectations not being met	Single breech in statutory duty Challenging external recommendations Local media interest Claims between £10,000 and £100,000 Formal complaint expected Impacts on small number of the population	Multiple breaches in statutory duty Legal action certain between £100,000 and £1million Multiple complaints expected National media interest	Multiple breaches in statutory duty Legal action certain amounting to over £1million National media interest Zero compliance with legislation Impacts on large percentage of the population Gross failure to meet national standards

Risk Grading Descriptors

LIKELIHOOD DESCRIPTION	
5 Almost Certain	Likely to occur, on many occasions
4 Likely	Will probably occur, but is not a persistent issue
3 Possible	May occur occasionally
2 Unlikely	Not expected it to happen, but may do
1 Rare	Can't believe that this will ever happen