NHS Wales
Internet Use Policy

Author: Information Governance Management Advisory Group Policy Sub Group
Approved by: Information Governance Management Advisory Group
Approved by: Wales Information Governance Board
Version: 2
Date: 06/09/2018
Review date: 06/09/2021

This Page is intentionally blank

Contents

1. Introduction

This document is issued under the All Wales Information Governance Policy Framework and maintained by the NHS Wales Informatics Service (NWIS) on behalf of all NHS Wales organisations.

2. Purpose

This policy provides assurance that 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 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 the workforce of all NHS Wales organisations including staff, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of NHS Wales.

For the purpose of this policy 'NHS Wales Organisations' will include all NHS Wales organisations including all Health Boards and NHS Trusts.

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.

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.

4. 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 Data Protection Officer, Senior Information Risk Officer and the Caldicott Guardian 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.

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. Breaches of this policy must be reported via local incident reporting processes.

5. Policy

5.1 Position 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 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.

5.2 Conditions & Restrictions

To avoid inadvertent breaches of this policy, inappropriate content 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 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.

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 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 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 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.

5.3 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 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.

Where local organisations have 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 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.

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 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.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact their local information governance department.

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

7. Monitoring and compliance

NHS Wales trusts its workforce.

NHS Wales reserves the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that the employee practices in work may come under scrutiny. NHS Wales

organisations respect the privacy of its employees and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

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, however it reserves 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 employees 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 counter fraud team.

In order for NHS organisations 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 IG 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 every two 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.

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 - 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.
- 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 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 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;
        - 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 All Wales Disciplinary Policy.

Annex 1: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
01/2017	V1	Andrew Fletcher (on behalf of the Internet and Email policy sub group)	Original policy as approved January 2017
12/09/2017	V1.1	Andrew Fletcher (on behalf of the IGMAG policy sub group)	Policy text applied to new template. Duplicate and substitute statements replaced with template text except insofar as they were not covered by these statements.
05/10/2017	V1.2	Andrew Fletcher (on behalf of the IGMAG policy sub group)	Comments from IG Leads in sub group applied to the policy.
04/12/2017	V1.3	Andrew Fletcher (on behalf of the IGMAG policy sub group)	Comments from IM&T Leads applied to the policy.
10/01/2018	V1.4	Andrew Fletcher (on behalf of the IGMAG policy sub group)	IGMAG Policy Sub Group changes applied to the policy.
07/02/2018	V1.5	Andrew Fletcher (on behalf of the IGMAG policy sub group)	Comments from all IG Leads applied. Draft for approval
08/03/2018	V1.6	Andrew Fletcher (on behalf of IGMAG)	Version control information updated
30/04/2018	V1.7	Andrew Fletcher (on behalf of IGMAG)	Version control information updated – No changes following Welsh Partnership Forum Consultation.
08/05/2018	V1.8	Andrew Fletcher (on behalf of IGMAG)	Changes following Equality Impact Assessment. Completed equality impact assessment added.

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
07/02/2018	V1.4	IGMAG Policy sub group	Sub group of the Information Governance Management and Advisory Group
08/03/2018	V1.5	Information Governance Management and Advisory Group	All Wales Information Governance Leads
30/04/2018	V1.6	Welsh Partnership Forum	All Wales workforce leads and trade unions
08/05/2018	V1.7	Equality Impact Assessment	NWIS Equality Impact Assessment Group
07/06/2018	V1.8	Information Governance Management and Advisory Group	All Wales Information Governance Leads
26/06/2018	V1.8 for approval	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)

Approvers

This document requires the following approvals:

Date	Version	Name	Position
07/06/2018	V1.8	Information Governance Management and Advisory Group	All Wales Information Governance Leads
26/06/2018	V2	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)

Annex 2: Equality Impact Assessment

Equality Impact Assessment (EQIA) Form	
Ref no: POL/IGMAG/Internet Use/v1	
Name of the policy, service, scheme or project:	Service Area
NHS Wales Internet 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 the Health Boards and NHS Trusts.
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

Key	
✓	Yes
x	No
-	Neutral

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?							✓				

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 **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**	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.

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 breeches in statutory duty Legal action certain between £100,000 and £1million Multiple complaints expected National media interest	Multiple breeches 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