CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

NHS Wales
Email 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
18/09/2020	D0.1	Francesca Harries	Initial draft developed supplementary to the All Wales Email Policy V3
21/09/2020	D0.2	Jeannette Short	Updates
21/09/2020	D0.3	Jeannette Short	Updates following review by Darren Lloyd
22/09/2020	D0.4	Jeannette Short	Final Draft
23/09/2020	V1	Jeannette Short	
13/09/2021	Draft V1.1	Sarah Muirhead	Update from NWIS to DHCW 'SFSP' link updated to 'Move-It – Self Service Portal'
03/03/2022	V1.2	Sarah Muirhead	Changed date on front page/Footer. Added Bullet Point and changed 'Employee' to 'Staff Member'
16/03/2022	V1.3	Francesca Harries	Updates following review by Jeannette Short
14/04/2022	V2.0	Francesca Harries	

Reviewers

This document requires the following reviews:

Date	Version	Name	Position
21/09/2020	V0.2	Darren Lloyd	Head of Information Governance, DHCW
14/03/2022	V1.2	Jeannette Short	Primary Care Support and IG Assurance Manager, DHCW
25/03/2022	V1.3	Darren Lloyd	Associate Director of Information Governance & Patient Safety, DHCW

Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name:	Jeannette Short
Role:	Primary Care Support and IG Assurance Manager
Signature:	14/04/2022 X Jeannette Short Jeannette Short Primary Care Support and IG Assurance Man... Signed by: Francesca Harries (Fr215649)

Approver's Name:	Darren Lloyd
Role:	Associate Director of Information Governance & Patient Safety

Signature:	14/04/2022 X  Darren Lloyd Associate Director of Information Governan... Signed by: Francesca Harries (Fr215649)

Contents

1. Introduction

This document is supplementary to the All Wales Email 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 email facilities are being used appropriately to assist in delivering services.

The policy also sets out the responsibilities of all users when using NHS Wales Email Services. 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 email 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 the NHS Wales Email Service via the NHS Wales network infrastructure.

The term 'staff' includes all health professionals, partners, staff member, 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 providing primary care services on behalf of NHS Wales.

This policy applies to all those making use of the NHS Wales Email Service by any means regardless of the location from which accessed, and the type of equipment used, for example corporate equipment, devices owned by a third-party organisation or personal devices operated under a Bring Your Own Device Scheme (BYOD).

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 Organisations 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. Inappropriate Emails

Inappropriate content and material must not be sent by email. Inappropriate content including prohibited language in emails may be blocked. Subject matter considered inappropriate is detailed in Appendix B.

Regardless of where accessed, users must not use the NHS Wales email system to participate in any activity, to create, transmit or store material that is likely to bring NHS Wales into disrepute or incur liability on the part of the Organisation.

Some users may need to send and receive potentially offensive material as part of their role (for example - child protection). Users should request authorisation from their Senior Responsible Person prior to sending potentially offensive information through the NHS Wales Email Service. Users must also be mindful of the recipients of this type of information and should not store such information within the NHS Wales Email Service.

5.2. Personal Data and Business Sensitive Information: Filtering and Misdirection

The NHS Wales network is considered to be secure for the transfer of any information including personal data and business sensitive information within NHS Wales, NHS England, and organisations with Transport Layer Security (TLS) enabled. This includes all email addresses within the NHS Wales Email Directory that end in “wales.nhs.uk”, which are hosted on the NHS Wales Email Service. Emails that are hosted by NHS England that end in “nhs.net” are also considered secure, however as users of the NHS Wales Email Network do not have access to NHS England’s Email Directory, extra vigilance MUST be made to ensure the correct email address is used. Email services of TLS enabled organisations as listed on HOWIS are also considered secure to communicate with, again extra vigilance should be applied when entering the email address to avoid misdirection. The list can be accessed here: TLS Assurance (sharepoint.com).

Transfer of personal data or business sensitive information between any email address not ending in “wales.nhs.uk”, “nhs.net” or TLS enabled, is not currently considered secure. Where this type of information needs to be sent, appropriate security measures must be implemented, for example, the information should be sent via the MoveIT secure file sharing portal or via email with an appropriate level of encryption.

Users must be vigilant in ensuring that all emails are sent to the correct recipient and must check that the correct email address is used, for example by checking the NHS Wales Email Address Book within Outlook. Even where the recipient email address is considered secure, as a mitigating factor to avoid any inadvertent misdirection, encryption of any email attachment containing sensitive data should be considered. Misdirected emails should be reported via local incident reporting processes.

5.3. Personal Use

NHS email accounts must not be used as a personal private email account.

Private use of email is permitted in the following circumstances:

- Emails to occupational health;

- Email for Health and Wellbeing;
- Communications connected with approved personal development / training;
- Communications with Trade Unions and Professional Bodies;
- Emergency emails.

Users must not subscribe to or provide any NHS email address to any third-party organisation for personal use.

5.4. Access to Information Requests

Information held on computers, including those held in email accounts may be subject to requests for information under relevant legislation and regulation. All staff should be mindful that it may be necessary to conduct a search for information and this may take place with or without the author's knowledge or consent.

5.5. Records Management

The NHS Wales Email system must not to be used as a storage facility.

- All emails should either be deleted or saved securely to the appropriate record (e.g. to a clinical / business record or network drive).
- Any emails that are retained within the email system will be automatically archived by the email system.

Note: At the time of writing, the Email Retention Policy is set for 7 years, with legal hold. A national programme of work is currently considering further agreement on specific retention periods; this policy will be updated to reflect such as national records management policies are set.

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.

The workforce of the Organisation should become competent in using NHS Wales Email 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 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.

NHS Wales uses software to scan emails for inappropriate content and filters are in place to detect this. Where an email is blocked, emails may be checked for compliance when a user requests an email to be

released. All email use will be logged to display date, time, username, email content; and the address to which the message is being sent.

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. 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 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 – 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, staff members, 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:

- Knowingly using another person's NHS Wales email account and its functions or allowing their email account to be used by another person without the relevant permission. Note: If an email is required to be sent on another person's behalf then this must be performed using delegated permissions functionality and must be approved for use beforehand;
- Allowing access to NHS Wales email services by anyone not authorised to access the services, such as by a friend or family member;
- Communicating or disclosing confidential or sensitive information unless appropriate security measures and authorisation are in place;
- Communicating or saving 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.
- Knowingly breaching copyright or Intellectual Property Rights (IPR)
- 'Hacking' into others' accounts or unauthorised areas;
- Obtaining or distributing unlicensed or illegal software by email;
- 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);
- Deliberately disabling or overloading any ICT system or network, or attempting to disable or circumvent any system intended to protect the privacy or security of employees, patients or others;
- Intentionally introducing malicious software such as Viruses, Worms, and Trojans into the NHS Wales network;
- Expressing personal views that may bring NHS Wales into disrepute;
- Distributing unsolicited commercial or advertising materials;
- Communicating unsolicited personal views on political, social, or religious matters with the intention of imposing that view on any other person. This does not preclude Trade Union officials from communicating with staff on Trade Union related matters;
- Installing additional email related software, or changing the configuration of existing software without appropriate permission;
- Sending unlicensed or illegal software or data including executable software, such as shareware, public domain and commercial software without correct authorisation;
- Forwarding chain email or spam (unsolicited mail) within the organisation or to other organisations;
- Subscribing to a third-party email notification using a NHS Wales email account for reasons not connected to work, membership of a professional body or trade union;
- Sending personal photos or videos;
- Registering a NHS Wales e-mail address with any third party company for personal use (e.g. department store accounts; online grocery shopping accounts);
- 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;
    - 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.

Annex 1: Equality Impact Assessment

Note: This EQIA has been taken from original All Wales Email Policy

Equality Impact Assessment (EQIA) Form		
Ref no: POL/IGMAG/Email Use/v2		
Name of the policy, service, scheme or project:	Service Area	
NHS Wales Email Use Policy	Information Governance	
Preparation		
Aims and Brief Description	The policy maintains the aim of having a single Email Use Policy for all NHS Wales organisations, to promote the same principles and values across all NHS Wales organisations and its workforce.	
Which Director is responsible for this policy/service/scheme etc	n/a 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 email 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 Email 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 email 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