



# NHS Wales Email 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:** 3

**Date:** 4<sup>th</sup> October 2019

**Review date:** 26<sup>th</sup> June 2020

**This Page is intentionally blank**

# Contents

- 1. Introduction ..... 4**
- 2. Purpose..... 4**
- 3. Scope ..... 4**
- 4. Roles and responsibilities ..... 4**
- 5. Policy ..... 5**
  - 5.1 Inappropriate emails ..... 5**
  - 5.2 Personal Data and Business Sensitive Information: Filtering and Misdirection ..... 5**
  - 5.3 Personal Use..... 5**
  - 5.4 Access to Information requests ..... 6**
- 6. Training and Awareness ..... 6**
- 7. Monitoring and compliance ..... 6**
- 8. Review..... 7**
- 9. Equality Impact Assessment..... 7**
- Appendix A - Inappropriate use ..... 8**
- Annex 1: Policy Development - Version Control ..... 9**
- Annex 2: Equality Impact Assessment..... 10**

## 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 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 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 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.

This policy applies to all those making use of the NHS email services 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.

## 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 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 A.

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 NHS Wales organisations.

Some users may need to receive and send potentially offensive material as part of their role (for example - child protection). Arrangements must be authorised to facilitate this requirement.

### 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 and organisations with Transport Layer Security (TLS) enabled. This includes all email addresses within the NHS email directory that end in "wales.nhs.uk", which are hosted on the NHS Wales email service and the email services of TLS enabled organisations as listed on HOWIS. The list can be accessed here: <http://howis.wales.nhs.uk/sites3/page.cfm?orgid=852&pid=74727>.

Transfer of personal data or business sensitive information between any email address not ending in "wales.nhs.uk", 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 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. 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.

Please note: where local organisations have provided patients and staff with access to public Wi-Fi services, staff may use these to access personal email accounts on their own device in their own time.

## 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 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 should be automatically archived by the email system. This data should not be retained for any period of time greater than 6 years.

## 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 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 trusts its workforce, however it 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 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 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. 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 the 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 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 - 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: Policy Development - Version Control

### Revision History

Date	Version	Author	Revision Summary
26/06/2018	V2	Andrew Fletcher (on behalf of the Internet and Email policy sub group)	Original policy as approved by WIGB June 2018
19/08/2019	V2.1	Andrew Fletcher (on behalf of the Internet and Email policy sub group)	Changes made to section 5.2 to reflect the implementation of transport layer security
05/09/2019	V2.2	Andrew Fletcher (on behalf of the Internet and Email policy sub group)	Version for approval

### Reviewers

This document requires the following reviews:


Date	Version	Name	Position
08/05/2018	V1.7	Equality Impact Assessment	NWIS Equality Impact Assessment Group
19/08/2019	V2.2	IGMAG Policy sub group	Sub group of the Information Governance Management and Advisory Group
05/09/2019	V2.2	Information Governance Management and Advisory Group	All Wales Information Governance Leads
	V2.2	Welsh Partnership Forum	All Wales workforce leads and trade unions
	V2.2 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
05/09/2019	V2.2	Information Governance Management and Advisory Group	All Wales Information Governance Leads
		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/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 it's 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?	<p>Yes. A sub group has developed this policy with a membership consisting of information governance leads and an OSSMB representative. IM&amp;T leads and the Wales Partnership Forum have been consulted.</p> <p>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.</p>
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 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
<b>To eliminate discrimination and harassment</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Promote equality of opportunity</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Promote good relations and positive attitudes</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Encourage participation in public life</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>In relation to disability only, should the policy / service / project or scheme take account of difference, even if involves treating some individuals more favourably?</b>	✓										



## 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:	<b>Yes</b>	<b>No</b>	<b>N/A</b>
<b>Article 2: The Right to Life</b>	X		
<b>Article 3: the right not to be tortured or treated in a inhumane or degrading way</b>	X		
<b>Article 5: The right to liberty</b>	X		
<b>Article 6: the right to a fair trial</b>	X		
<b>Article 8: the right to respect for private and family life</b>	X		
<b>Article 9: Freedom of thought, conscience and religion</b>	X		
<b>Article 14: prohibition of discrimination</b>	X		

## Measuring the Impact

What operational impact does this <b>policy, service, scheme or project</b> , have with regard to the Protected Characteristics. Please cross reference with equality duties	
	<b>Impact – operational &amp; financial</b>
<b>Race</b>	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.
<b>Sex/gender</b>	
<b>Disability</b>	
<b>Sexual orientation</b>	
<b>Religion belief and non belief</b>	
<b>Age</b>	There is a clear statement around behaviours making it explicit that hateful and discriminatory language will not be accepted.
<b>Gender reassignment</b>	
<b>Pregnancy and maternity</b>	There needs to be a wider understanding and context of trigger words.
<b>Marriage and civil partnership</b>	
<b>Other areas</b>	
<b>Welsh language</b>	Dignity and respect of those using email policy as individuals and staff and clear instructions so staff know what is applicable to them.
<b>Carers</b>	

## Outcome report

<b>Equality Impact Assessment: Recommendations</b>		 			
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	AF	ASAP	Time	
2	Updated EQIA statement	AF	ASAP	Time	

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

## Risk Assessment based on above recommendations

<b>Reputation and compromise position</b>		<b>Outcome</b>	
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.	
<b>Training and dissemination of policy</b>			
The policy is clear so that all staff aware of responsibilities and therefore reputation of organisation is preserved.			
<b>Is the policy etc lawful?</b>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	<b>Review date</b>	
<b>Does the EQIA group support the policy be adopted?</b>	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	<b>3 years</b>	

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
	<b>Negligible</b>	<b>Minor</b>	<b>Moderate</b>	<b>Major</b>	<b>Catastrophic</b>
<b>Statutory duty</b>	No or minimal impact or breach of guidance / statutory duty  Potential for public concern  Informal complaint  Risk of claim remote	Breach 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 breach 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