GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW83 **Version Number:** 1.0 **Date of next review:** May 2026

EMAIL ACCEPTABLE USE POLICY

Policy Statement

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

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

Policy Commitment

Email is provided to staff to assist them in the performance of their duties and the provision of these facilities represents a major commitment on the part of NHS Wales in terms of investment and resources. The NHS Wales workforce should be competent in using email to the level required for their role in order to be efficient and effective in their day-to-day activities. Public Health Wales will support its workforce in understanding how to safely use email and it is important that users understand the legal, professional and ethical obligations that apply to its use. If used correctly, email can increase business efficiency and service user safety.

Supporting Procedures and Written Control Documents

All Wales Information Governance Policy

Scope

This policy applies to all staff 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.

Equality and Health Impact Assessment	EHIA IG Policies Jan 2024.docx.

Approved by	Audit and Corporate Governance Committee
Approval Date	09/05/2024
Review Date	1/5/2026
Date of Publication:	
Group with authority to approve supporting procedures	Senior Leadership Team
Accountable Executive Director/Director	Iain Bell, Senior Information Risk Owner and National Director of Public Health Knowledge and Research
Author	John Lawson, Head of Information Governance

Disclaimer

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

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
0.1	17/01/2024			New Policy to replace withdrawn All Wales Policy
1.0	01/05/2024	09/05/2024		

1. Introduction

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.

2. Roles and Responsibilities

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

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

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

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

3. Policy

Restrictions

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.

Personal use of the internet

NHS email accounts must not be used as a personal private email account. Private use of email is permitted in the following circumstances:

- Emails directly related to the health and wellbeing of the employee (e.g. occupational health);
- Communications connected with approved personal development / training;
- Communications with Trade Unions and Professional Bodies or is otherwise exercising a right provided by law relating to the workplace;
- Emails where the employee is dealing with a personal emergency and has no alternative method of communication immediately available.

Users must not subscribe to or provide any NHS email address to any third party organisation for personal use, other than in the circumstances outlined above.

Data subject rights and Freedom of Information

Everyone in the UK has a number of rights under data protection legislation in relation to information relating to them which is held by any organisation. Those rights include (but are not limited to):

- Right of access to their personal data;
- Right to have their personal data rectified if inaccurate;
- Right to restrict the processing of their personal data and
- Right to object to their personal data being processed.

Any email that relates to a living individual (including staff) and from which that individual can be identified is considered their personal data and so the rights outlined above will apply.

Also, as a public body Public Health Wales is subject to the Freedom of Information Act (FOIA), which means that any information contained in emails may be required to be disclosed following a FOIA request[1]. FOIA releases are considered as a 'release to the world' and are published on our intranet.

Staff must be aware that anything written in an email may become disclosable under either of the above provisions with or without the staff members knowledge or consent.

Sharing of personal data

Email and attachments to emails are not considered a secure method of sharing personal data due to the high incidence of emails being sent to the wrong recipient and must not be used unless no alternative method exists.

Wherever possible, internal sharing of personal data must be achieved through the use of Sharepoint, by sending links to documents that have appropriate access controls applied.

For external sharing the preferred method is Secure File Sharing Portal. Sharing by email must only be done by email with trusted partners who have TLS enabled email connectivity[2].

When sharing by email, either internally or to trusted external partners, any attachments containing personal data must be password protected and the password must be provided separately to the document, preferably by a different means (e.g. SMS).

In all cases it is the responsibility of the sender to ensure that the right information is shared with the right people, and that any sharing is done lawfully, fairly and safely. If in any doubt, staff should contact the Information Governance Service prior to sharing.

4. 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.

[1] Certain exemptions apply. Refer to the Freedom of Information Procedure for further details

[2] Transport Layer Security. For details of organisations currently approved refer to

5. Monitoring and compliance

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

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

Public Health Wales uses software to 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.

In addition, the Information Governance Service will from time to time search individual staff members emails in order to respond to data subject rights enquiries. This is in line with the Data Subject Rights Procedure and further information can be found in that document.

Staff should be reassured that NHS Wales organisations take a considered approach to monitoring, however it reserves the right to adopt such monitoring methods and patterns as may be deemed appropriate from time to time.

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

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

6. Records Management

The email system should 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.

7. Review

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

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

8. Equality Impact Assessment

This policy has been subject to an equality assessment.

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

Appendix A - Inappropriate use

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;
- 'Hacking' into others' accounts or unauthorised areas;
- Communicating or saving any information or images which are unlawful, or which without a legitimate business use would objectively 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.
- The use of language that suggests or implies any of the above is prohibited under this policy.
- Knowingly breaching copyright or Intellectual Property Rights (IPR)
- Knowingly obtaining or distributing unlicensed or illegal software by email;
- Deliberately attempting to circumvent security systems protecting the integrity of the NHS Wales network;
- Any activity that knowingly or recklessly denies service to other users (for example, deliberate or reckless overloading of access links or switching equipment);
- Knowingly or recklessly 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.