NHS Wales
All Wales Email Use Policy

Issue Date: 7 January 2016
Review Date: 7 January 2018

1 DOCUMENT HISTORY

1.1 Revision History

Date	Version	Author	Revision Summary
7/9/15	V0.87	Andrew Fletcher / Darren Lloyd, NWIS (on behalf of the Internet and Email policy sub group)	Final Draft
29/9/15	V0.88	Andrew Fletcher / Darren Lloyd, NWIS (on behalf of the Information Governance Management and Advisory Group)	Minor amendment (as a condition of approval)
1/12/15	V0.89	Andrew Fletcher / Darren Lloyd, NWIS (on behalf of the Information Governance Management and Advisory Group)	Minor amendments (as a result of Equality Impact Assessment)

1.2 Reviewers

This document requires the following reviews:

Date	Version	Name	Position
12/08/15	V0.86	Internet and Email policy sub group	Representation from all NHS Wales Information Governance, Information Security, Communications and Human Resources
29/09/15	V0.87	Information Governance Management and Advisory Group	All Wales Information Governance Leads
23/10/15	V0.88	Wales Information Governance Board	Advisory Board to the Minister for Health and Social Care (Welsh Government)
1/12/15	V0.89	Equality Impact Assessment Panel	Independent equality impact assessment
3/12/15	V1	Welsh Partnership Forum	

Scope

This policy applies to all users of the NHS Wales email system including staff; students; trainees; secondees; volunteers; and contracted third parties including locum and agency staff.

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.

Position Statement

NHS Wales trusts its workforce when using NHS Wales equipment.

Email functionality 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 email services to the level required of their role in order to be efficient and effective in their day-to-day activities.

Staff should be aware that the email system is not to be used as a facility for permanent retention of documentation. Business content in email messages and any attachment that need to be retained must be saved to the appropriate functional area of the corporate management filing system.

NHS Wales will support its workforce in understanding how to safely use email services and it is important that users understand the legal professional and ethical obligations that apply to its use. If used correctly, email systems can increase efficiency and safety within patient care. Risks can be reduced by utilising email as an established form of NHS and patient communication.

Inappropriate emails

Inappropriate content and material must not be sent by email. Inappropriate content including prohibited language in emails may be blocked. For the avoidance of doubt, subject matter considered inappropriate to send is detailed in appendix A.

In general, regardless of where accessed (for example - at work or at home), NHS Wales employees must not, at any time, use the NHS Wales email system to participate in any activity or to create or transmit or store material that is likely to bring NHS Wales into disrepute or incur liability on the part of NHS Wales organisations.

Staff must not subscribe to or provide their NHS email address to third parties for personal use.

Some staff members may need to receive and send potentially offensive material as part of their role (for example - child protection). Arrangements will be in place to anticipate this requirement.

Personal Identifiable Information and Business Sensitive Information - Filtering and Misdirection

The NHS Wales network is considered to be secure for the transfer of any information including PII and business sensitive information. This includes all email addresses in the NHS email directory which include those email addresses typically end in “wales.nhs.uk” and “Powys.gov.uk” (which is hosted on the NHS Wales email service).

Photographs and video recordings of patients, members of the public, or other members of staff taken on NHS Wales premises must not be sent by email unless this is part of the senders duties and local processes have been followed.

Transfer of personal identifiable information or business sensitive information to a public service (e.g. “.gov.uk”), partner organisations and NHS services within other parts of the UK (i.e. to email addresses ending in “scot.nhs.uk” or “hscni.net” or “nhs.net” “or nhs.uk”) is not currently considered secure. Where this type of email needs to be sent steps must be taken to risk assess the situation and appropriate security measures must be put in place unless the risk is outweighed by any risk to a patient or clients’ health and wellbeing. If content of the email is deemed sensitive additional secure protection should be put in place (for example sending the information as an encrypted attachment).

Where a regular transfer of personal identifiable information to non-NHS partner organisations is to be made this should be managed within a documented procedure that minimises the risk of unauthorised disclosure or loss and which complies with the regulations set out in the Wales Accord on the Sharing of Personal Information (WASPI) framework.

The PII of an employee must only be forwarded to that employee’s own non-NHS Wales email account (by HR for example) at their request and only after the risks have been explained fully and consent is given to receiving information in this way. Full detail of this process followed should be recorded.

Email has a higher chance of interception when sending outside of the NHS Wales network and therefore a set of rules is in place that aims to identify personal identifiable information (PII) and confirm any sending activity with the user to avoid misdirection. While it is recognised that email can be a quicker way of communicating PII, staff should be aware that there are other methods of sending person identifiable information, such the Secure File Sharing Portal (SFSP) should be used for the routine sending of PII outside of NHS Wales.

Users must be vigilant in ensuring that all emails are sent to the correct recipient and to use the NHS address book to check that the correct email address or addresses have been selected. If you receive a misdirected email you must report this to your local information governance / security department.

Personal Use

NHS Wales organisations allow staff reasonable personal use of email services providing this is within the bounds of the law and decency and complies with policy. Ordinarily the NHS email account should not be used routinely as a person’s private email account

Personal use should be incidental or reasonable and before or after normal working hours, or during agreed break times. These limitations are also necessary due to network demands and therefore users must not send large files when using the email system in a personal capacity as these may have a negative impact on network resources including bandwidth and storage.

Where local organisations have provided patients and staff with cloud internet services (for example - public wireless network functions (Wi-Fi)) to access the public internet this should be used by staff for personal private use to personal email accounts on personally-owned devices where this is possible.

Monitoring

NHS Wales organisations reserves the right to monitor emails of any user. NHS Wales uses software to scan emails for inappropriate content and filters are in place to detect the sending of PII outside of the NHS Wales network. All email use will be logged to display date, time, username; and the address to which the message is being sent. This will inevitably mean that email accounts which are used for personal reasons could potentially be monitored and accessed.

Staff should be reassured that NHS Wales organisations take a considered approach to monitoring individual usage of the email system. Monitoring is normally conducted on the basis that such usage is suspected to be in breach of either a NHS Wales policy or legislation. On deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

All audit and monitoring reports will be retained in line with NHS Wales retention and disposal schedules and Department for Health and Social Care Guidance. Additional audits or monitoring reports can be requested by line managers and activated in the system with the agreement of the relevant Head of Service. Emails may be automatically archived by the email system. This data should not be retained for any period of time greater than 6 years.

Reporting breaches of this policy

Breaches to this policy must be managed in line with the All Wales Disciplinary Policy.

Any illegal activity such as fraud, or corruption carried out in using the email system will be reported to the appropriate authorities.

Subject Access and Freedom of Information Act requests

Information held on computers, including those held in email accounts may be subject to requests for information under the Data Protection Act 1998 (Principle six: Subject Access) or under the Freedom of Information Act 2000 (Freedom of Information Act Requests). All staff should be mindful that it may be necessary to conduct a search for information.

Governance and Review arrangements

This document is issued and maintained by the NHS Wales Informatics Service (NWIS) on behalf of organisations in NHS Wales and shall be reviewed on a two yearly basis by:

The NHS Wales Information Governance Management Board
The Wales Information Governance Board; and

The Welsh Partnership Forum

This policy will be reviewed as per the review date on the policy front sheet; however it will be reviewed particularly where they are affected by major internal or external changes such as:

- Changes in Legislation;
- Practice change or change in system/technology; or
- Changing methodologies.

Training

Training relating to this policy must take place during the induction programme for new staff or as part of refresher training at least every two years as part of the Information Governance and Information Security training.

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. 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 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 unless appropriate security measures and authorisation are in place;
- Communicating any information which could be regarded as offensive or inappropriate. This includes that which can be reasonably deemed to be undesirable, defamatory, abusive, hateful, racist, sexist, homophobic, transphobic, discriminatory, indecent, obscene, pornographic, unlawful or involves violence, bullying or harassment.
- Communicating or disclosing material that is intended to distress, annoy or intimidate another person or is contrary to the Organisation’s Dignity at Work Policy;
- Sending or saving information or images which could be considered defamatory, obscene, hateful, pornographic, violent, terrorist, racist, sexist, homophobic, transphobic or otherwise illegal material.
- 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 your 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;
    - The Doctors.net email service;
    - 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.