Ref: IG 03
Email and Instant Messaging (EIM) Use Policy

Executive Sponsor and Function:	Executive Director of Finance
Document Author:	Head of Information Governance
Approved by:	Quality, Safety and Performance Committee
Approval Date:	7th May 2026
Date of Equality Impact Assessment:	20th October 2025
Equality Impact Assessment Outcome:	Approved - 5th February 2026
Review Date:	May 2029
Version:	1

Contents

1. Aim

The aim of this Policy is to set out the key areas of responsibilities and the Trust's commitment to ensuring the organisation uses Email and Instant Messaging lawfully and correctly.

For the purposes of this Policy, the Trust takes the view that the principles of confidentiality continue to apply to the use of Email and Instant Messaging in respect of information including commercial data, and all personal data, whether employee, patient, donor and/or service user.

The policy also aims to provide all employees of the Trust with a framework in which to ensure that the use of email and instant messaging is conducted lawfully and in conjunction with this policy.

2. Policy Statement and Objectives

The Email and Instant Messaging Policy (EIM) policy provides direction as to how NHS Wales Corporate EIM must be used.

This policy also sets out the roles and responsibilities of those using NHS Wales Corporate EIM services. These responsibilities include, but are not restricted to, ensuring that:

- The confidentiality, integrity, availability and suitability of information, NHS computer systems and third-party systems are maintained by ensuring use of EIM services is governed appropriately.

- All those identified within the scope of this policy are aware of their obligations in accordance with legislation, standards, guidance and Organisational policy.

This Policy sets out the high level intent of the Trust and also recognises the diversity of the respective Divisions and associated organisations under its control. This policy must be read in conjunction with all relevant national policies, which includes but is not exclusive to the Trust's Information Governance Policy

3. Scope

This policy applies to the workforce of all Velindre University NHS Trust staff, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of NHS Wales. Thereafter defined as "*EIM Users*".

This policy applies to all EIM Users, regardless of access location, device type (e.g., corporate, third-party, or personal BYOD), or access method.

Corporate EIM solutions include NHS Wales systems such as NHS Wales Email, NHS Wales Microsoft 365 platform and MS Teams. This Policy does not include Non-Corporate Communication Channels

(NCCC) which includes Instant Messaging services such as WhatsApp, Telegram, Cisco Webex, Facebook Messenger, We Chat etc. It is to be noted that unsupported and non-endorsed IM systems, such as those identified above must not be used for business purposes unless sanctioned for use by the individual organisation.

4. Roles and Responsibilities

This policy applies to all employees and contractors working for, or on behalf of the Trust. Everyone working for or with the NHS who records, handles, stores, or otherwise comes across information has a personal common law duty of confidence to individuals referred to in that information.

The Chief Executive Officer as the Accounting Officer of the Trust has overall responsibility for ensuring compliance with applicable legislation and regulation. Specific responsibilities will be delegated to the Data Protection Officer, Senior Information Risk Owner and the Caldicott Guardian or an Executive Director as appropriate.

Directors / Managers of Hosted Bodies and Divisions are responsible for the implementation of this policy within their area of responsibility. 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 and Cyber Security training.

Breaches of this policy must be reported via local incident reporting processes and dealt with in line with the All Wales Disciplinary Policy where appropriate.

EIM Users must familiarise themselves with policy content and ensure that policy requirements are implemented and followed within their own work area. Mandatory Information Governance training must be undertaken upon appointment and at least every two years thereafter.

The effectiveness of this Policy will be monitored by each Organisation's Corporate Governance function supported by their Information Governance Team.

5. Policy

5.1 Position Statement

All corporate emails and instant messaging (IM) are monitored to allow enforcement of this policy via Digital Teams using authorised software.

Corporate EIM facilities must only be used lawfully and must not be used for sending defamatory communications, or for harassment, unauthorised purchases, or for publishing views and opinions (defamatory or otherwise) which may lead NHS Wales into disrepute.

Corporate EIM only may be used for the communication of confidential information in line with applicable legislation such as the UK General Data Protection Regulation (UK GDPR), Freedom of Information Act 2000, ICO Guidance and Health Board/Trust/Special Health Authority policies and procedures.

The use of email to communicate personal data is a last resort, and any data that includes personal data must be sent via the All Wales Secure File sharing Portal. If this is not possible all personal data must be encrypted prior to sending, and the password communicated securely to the recipient. This requirement is mandatory for all patient and staff information. Local Digital and IG teams can supply an up to date list of approved secure email domains and systems for sending personal data.

This Policy does not consider the use of Non-Corporate Communication Channels (NCCCs) and personal email accounts. Staff are to note that business information contained within personal email accounts and NCCCs remain subject to applicable UK Data Protection Legislation.

Any use of NCCCs must be authorised by the Trust through the Information Governance Team and a register kept of NCCC Groups.

Users must be diligent when using EIM facilities to ensure intended recipients are selected for that communication, this is essential to avoid misdirection of data. A breach as a result of misdirection must be reported within DATIX Once for Wales (OFW) in the same manner as any other incident within NHS Wales. Trust procedures and standards must be followed for best practice use of EIM facilities. Subject matters considered inappropriate are detailed in appendix A

5.2 Personal Use

NHS email accounts must not be used to send or receive personal / private emails, unless for one of the following purposes:

- 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 unless authorised or endorsed by your organisation.

6. Records Management

Information sent by corporate EIM may be subject to a request for information under the Freedom of Information Act 2000, the Environmental Information Regulations (EIR), Access to Health Records Act,

or Data Protection legislation and therefore should be managed in accordance with the organisations records management policy and any accompanying procedures.

The corporate EIM system itself **must** not to be used as a storage facility. The following practice must be followed in relation to EIM:

- All EIM should either be deleted or saved securely to the appropriate record (e.g. to a clinical / business record, SharePoint or network drive).
- Any EIM emails that are retained within the email system will be automatically archived by the EIM system. This data is then retained for a period of 7 years.

7. Access to EIM under Information Request Procedures

Information held on computers, including those held in EIM 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 relevant information to respond to the request, and that the author's consent or knowledge is not required such search activity.

8. Monitoring and Compliance

The Trust reserves the right to monitor and audit activity in business premises, use of business facilities and working practices of its employees to ensure compliance with this policy, legislative requirements and the effectiveness of services provided.

It includes monitoring and auditing equipment such as CCTV systems, access control entry systems and any ICT equipment used in the service.

When monitoring employee activity, the Trust will assess:

- The purpose of the auditing and what it aims to achieve
- Whether the processing of personal information is necessary to fulfil the purpose of the monitoring, whilst at the same time ensuring that the business interests that monitoring seeks to protect are legitimate
- Whether the monitoring is lawful, both generally and in particular when considering data protection law
- Whether consideration of the information rights of employees has been appropriately considered (a balancing test)

The tools used for monitoring will be used according to the purpose that has been clearly defined. Data that is processed must be kept secure and access to the data must be lawful.

To ensure compliance with this policy all corporate EIM is monitored to allow for enforcement of this policy. Any suspected security breaches or unauthorised access must be reported immediately to the Trust's Data Protection Officer and the Digital Helpdesk.

Where a breach has occurred an audit of activity will take place to ascertain root causes, this may result in the extraction of corporate EIM without the knowledge of the Staff member.

9. Training, Awareness and Practical Considerations

The Trust demonstrates that employees understand their responsibilities to ensure that personal information is protected and processed in accordance with the applicable procedures, taking into account the related security requirements.

Section 8 of the Trust's Data Protection and Confidentiality Policy details the provision of training in relation to the processing of personal data. Staff are to read that Policy in conjunction with this EIM Policy.

10. Complaints

Anyone whose data is processed by the Trust is entitled to make a complaint if they are unhappy with the way their data has been processed.

Data Protection complaints are that same as any other complaint, however, the individual handling the complaint will be the Head of Information Governance who may need to undertake an investigation into the facts surrounding the complaint prior to responding to the complainant.

Members of Staff are to provide the following address for any individual who wishes to complain to the Trust about how their data has been handled:

Mr Ian Bevan via
VelindreInformationGovernance@wales.nhs.uk
Head of Information Governance
Velindre University NHS Trust
2, Charnwood Court
Heol Billingsley
Parc Nantgarw
Cardiff / Caerdydd
CF15 7QZ
Tel / Ffon - 029 20196161

It should be noted that an individual has the right not to complain to the Trust, but to the Information Commissioner's Office (ICO) by writing to:

Information Commissioner's Office – Wales
2nd Floor
Churchill House
Churchill Way
Cardiff
CF10 2HH

Tel: 0330 414 6421
Email: wales@ico.org.uk

11. Governance and Reporting

Compliance with this policy (and supporting procedures) will be monitored by the Head of Information Governance. An internal audit on the Trust's arrangements in relation to the Act will be scheduled in line with the Trust's internal audit strategy.

For assurance, details on Data Protection and Confidentiality activity (including complaints) will be reported to the Quality, Safety and Performance Committee, as well as the Senior Information Risk Owner (SIRO).

An annual Caldicott review and audit will be carried out, by associated organisations within the Trust, in respect of the way patient and/or donor information is managed and recommendations for progress established.

The Trust notifies details of the personal data it processes to the Information Commissioner for inclusion on the register of Data Controllers. The notification is reviewed annually by the Trust. The register is maintained by the ICO and is available in the public domain for inspection by anyone.

The policy will be reviewed every 3 years, unless affected by major internal or external changes such as: Legislation; Practice change or change in system/technology; or Changing methodology.

12. References - Specific applicable Legislation and Standards

This Policy is written in accordance with current legislation as well as relevant codes of practice and standards that include, but are not limited to, the following:

Human Rights

- European Convention on Human Rights
- Human Rights Act 1998

Rights to Privacy

- Investigatory Powers Act 2016
- Protection of Freedoms Act 2012
- Lawful Business Practice Regulations 2000

Data Protection

- Data Protection Act 2018 (incudes UK GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records Act 1990 (where not superseded by Data Protection Legislation)
- Health & Social Care Act 2012
- Data (Use and Access) Act 2025

Online Privacy

- UK Privacy and Electronic Communications Regulations (PECR)
- UK Privacy and Electronic Communications Amendment 2012 (Cookie Law)

Relevant Codes of Practice and Standards include, but are not limited to, the following:

- Caldicott Principles
- Information Security ISO27001
- Information Commissioners Codes of Practice
- ICO's Employment Information Guidance
- Common Law Duty of Confidence

13. 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.

14. Contacts

For further advice and/or assistance on how to ensure individual, divisional and associated organisational compliance with this Policy, please contact: -

Ian Bevan
Head of Information Governance
Velindre NHS Trust HQ
2, Charnwood Court

Heol Billingsley
Parc Nantgarw
Cardiff
CF15 7QZ
Email – VelindreInformationGovernance@wales.nhs.uk
Tel – 029 2031 6161

15. Further Information

This Policy should be read in conjunction with the following Trust policies:

- Information Governance Policy
- Confidentiality Breach Reporting Policy
- Records Management Policy
- Freedom of Information Act Policy
- Data Quality Policy
- Information Security Policy
- Internet Use Policy
- Social Media Policy

Appendix A - Inappropriate use

For the avoidance of doubt, NHS Wales will generally consider any of the following inappropriate use, including but not limited to:

- Deliberately attempting to circumvent EIM controls protecting the confidentiality, integrity and availability of the NHS Wales network on NHS Wales owned equipment and services, and knowingly not reporting any suspected security breaches or unauthorised access.
- Using someone else's corporate EIM account without permission.
- Allowing access to NHS Wales email services by anyone not authorised to access the services, such as by a friend or family member.
- Sharing confidential or sensitive information without proper security measures and authorisation.
- Sending or saving unlawful, offensive, or inappropriate content, including defamation, harassment, or discrimination.
- Knowingly violating copyright or intellectual property rights.
- Obtaining or distributing illegal software via EIM.
- Deliberate attempts to bypass security systems protecting the network.
- Purposely overloading systems to disrupt service to other users.
- Disabling or overloading ICT systems or attempting to bypass security protections.
- Introducing malicious software, such as viruses or trojans, into the network.
- Sending unsolicited commercial or advertising emails.
- Sending unauthorised or illegal software or data through EIM.
- Forwarding chain emails or spam internally or externally.
- Subscribing to third-party notifications for non-work-related purposes using your work email.
- Sending and receiving personal material i.e. non-business related material via EIM unless covered within section 5.1.
- Accessing personal email services from NHS Wales devices and networks is prohibited for security reasons, except for services permitted by the organisation.
- Access to internet based EIM providers such as Gmail, Hotmail, Yahoo 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 EIM accounts (accounts ending .ac.uk);
  - Any email account hosted by a body which the employee continue 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
01/2017	V1	Andrew Fletcher (on behalf of the Internet and Email policy sub group)	Original policy as approved (v1)
26/06/2018	2	Andrew Fletcher (Chair of the IGMAG policy sub group)	Original policy as approved (v2)
14/01/2021	3	Andrew Fletcher (Chair of the IGMAG policy sub group)	Original policy as approved (v3)
26/09/2024	Draft v3.1	Daniel Owen (Chair of OSSMB)	Included Instant messaging and updated policy.
15/01/2025	Draft v3.2	Ian Bevan (Chair of IGMAG)	Review updated Policy and local assessment of risk
06/02/2025	Draft v3.3	Andrew Fletcher (Chair of IGMAG policy sub group) / Ian Bevan (Chair of IGMAG)	Consistency checking with agreed information governance policy positions
11/02/2025	Draft v3.4	Andrew Fletcher (Chair of IGMAG policy sub group) / John Sweeney (IG Manager DHCW)	Consistency checking with agreed information governance policy positions
11/03/2025	Draft v3.4	IG Leads – IGMAG	Review post update
10/06/2025	Draft v4.0	Ian Bevan (Chair of IGMAG)	Review and update
24/07/2025	DRAFT v5	Ian Bevan, HoIG, VUNHST	Convert to Trust Policy