3 November 2026

Dear

ATISN 26-0056 – File Metadata

Thank you for your request to the Welsh Government for information under the Freedom of Information Act (2000) received on 18 October 2026 relating to national digital-object integrity, metadata behaviour, document-handling protocols, and email-routing governance across NHS Wales bodies under Welsh Government oversight.

You requested the following:

Section 1 — systemic deployment of grouped OLE package wrappers (2015–2026) Across NHS Wales bodies, digital objects have appeared within statutory and internal disclosures that visually resemble PDF images but are technically grouped OLE "Package" wrappers. These objects:

1) Are stored internally as { EMBED Package … },

2) Retain full metadata even when visually disguised,

3) When field-code inspection (such as SHIFT+F9) is applied, these disguised visual objects lay bare their true nature: they are active OLE package wrappers that retain their underlying structural frames and metadata. Grouping the object successfully conceals the visual bounding box—making the package appear as a harmless, static image—yet it entirely fails to scrub the internal system identifiers. Upon inspection, these embedded wrappers expose hardcoded routing paths and network pointers (such as \\rs), directly unmasking the local machine or laptop of the specific manager who built or modified the file.

Please provide the following information for the period 2015–2026, covering all NHS Wales bodies under Welsh Government oversight, including NWIS and DHCW:

1.1 systemic deployment

Records showing how many times grouped OLE package wrappers have been deployed across NHS Wales systems for purposes including:

a) overwriting existing documents

b) replacing documents when staff leave
c) reconstructing or re-sequencing narrative continuity
d) masking original file origins
e) embedding alternative versions of documents
f) concealing metadata within statutory or internal responses

1.2 detection, reporting, and recording

Any:

a) detection logs
b) audit trails
c) information governance reports
d) metadata-related incident records
e) digital-object handling reviews

Showing how many times grouped OLE package wrappers were detected, escalated, recorded, or investigated between 2015 and 2026.

1.3 information governance usage examples Examples (not personal data) of scenarios where information governance teams across NHS Wales:

a) used grouped OLE package wrappers
b) embedded packages instead of standard PDF attachments
c) deployed image-wrapped objects within SAR or FOI responses
d) used OLE packages to replace or overwrite internal documents

1.4 governance, policy, and endorsement
All Welsh Government or NHS Wales policies, governance frameworks, or information governance procedures that permit or regulate the use of:

a) OLE package objects
b) Grouped embedded packages
c)Image-wrapped document objects
Within statutory or internal correspondence.

Please supply the document name, section, page, paragraph, line number, or a direct URL.

1.5 recorded senior governance awareness (2015–2026) Any records showing whether the following roles were formally aware of, briefed on, or notified about the use of grouped OLE package wrappers:

1) Head Of Legal and Risk (NWSSP)
2) Deputy Of Legal and Risk (NWSSP)
3) Chief Executives of NHS Wales Trusts
D) Welsh Government Digital Governance Leads
E) Welsh Government Escalation or Oversight Officials

This request concerns role-based awareness only.

Please also provide any records showing whether correspondence relating to OLE package wrappers was diverted, reclassified, or routed into automated ticketing systems such as Action Point, including routing to OD People Level 5.

Section 2 — email routing, Action Point diversion, and systemic throttling Multiple NHS Wales bodies utilise automated ticketing platforms (for example, Action Point) which can intercept, divert, or reclassify incoming correspondence. Given Welsh Government's national oversight role, please provide:

2.1 Welsh Government responsibility

Confirmation of whether Welsh Government:

a) sets national standards for Outlook or Exchange mail-routing rules
b) oversees automated connectors or integrations with Action Point
c) approves throttling or suppression mechanisms applied to high-volume senders
d) regulates domain-based or address-based diversion rules
e) oversees automated reclassification or redirection filters used by NHS Wales bodies

2.2 technical specifications
Any system documentation, routing specifications, configuration standards, architectural diagrams, or technical descriptions explaining how:

a) automated diversion
b) throttling
c) suppression
d) reclassification
Rules are applied to incoming email streams across NHS Wales.

2.3 reporting and recording requirements The official policy, procedure, or standard operating procedure governing:

a) reporting routing anomalies
b) logging automated diversion errors
c) auditing email interception or suppression
d) documenting ticketing mis-routing or mis-classification

Please supply the document name, section, page, paragraph, line number, or a direct URL.

2.4 senior oversight
Records of any:

a) technical audits
b) briefings
c) risk assessments
d) governance escalations
e) internal reviews

involving Welsh Government digital leadership relating to:

a) email diversion
b) routing anomalies
c) automated suppression
d) Action Point integration
e) systemic throttling of correspondence

Section 3 — internal recruitment and oversight gaps
3.1 internal appointment ratios

Statistical data showing the proportion of senior digital, governance, information-rights, or technical-leadership roles filled internally versus externally across NHS Wales bodies between 2015 and 2026.

3.2 oversight risks

Any governance reviews, risk assessments, or internal analyses evaluating whether high internal appointment ratios reduce external challenge or scrutiny of legacy technical practices such as:

a) grouped OLE package deployment
b) metadata-bearing embedded objects
c) automated email diversion or suppression

3.3 executive oversight and departures

Any risk assessments, governance papers, or internal reviews examining whether:

a) digital-object handling
b) metadata reconciliation
c) mail-routing transparency
d) information-governance compliance
e) document-management integrity

Were subjects of internal challenge, whistleblowing, or executive departure considerations between 2015 and 2026.

Response

The Welsh Government's published digital health strategies set broad strategic direction for secure and resilient digital infrastructure, national standards, interoperability and cyber governance across NHS Wales. They do not, however, set specific standards or approval arrangements for Outlook or Exchange mail-routing rules; integrations with Action Point; sender throttling or suppression; domain- or address-based diversion; or automated email reclassification and redirection filters.

These matters are therefore not prescribed through the published health digital strategies. Responsibility for the configuration and operation of such controls would need to be confirmed with the relevant NHS Wales organisations and the provider of the national Microsoft 365 and Exchange service.

We have reviewed the relevant published digital health strategies. They do not contain specific guidance or requirements relating to the matters listed at (a) to (e).

The strategies provide an overarching framework for digital standards, infrastructure and cyber security, but do not prescribe detailed arrangements for email routing, filtering, throttling, redirection or integrations of the type described in the request.

You may wish to contact the various NHS organisations directly and their contact details can be found here

Next Steps

The request you sent me contains personal information about you - for example, your name and address. The Welsh Government will be the data processor for this information and, in accordance with the General Data Protection Regulation, it will be processed in order to

fulfil our public task and meet our legal obligations under the Act to provide you with a response.

We will only use this personal information to deal with your request and any matters which arise as a result of it. We will keep your personal information and all other information relating to your request for three years from the date on which your request is finally closed. Your personal information will then be disposed of securely.

Under data protection legislation, you have the right:

- to be informed of the personal data we hold about you and to access it
- to require us to rectify inaccuracies in that data
- to (in certain circumstances) object to or restrict processing
- for (in certain circumstances) your data to be 'erased'
- to (in certain circumstances) data portability
- to lodge a complaint with the Information Commissioner's Office (ICO) who is our independent regulator for data protection

For further information about the information which the Welsh Government holds and its use, or if you wish to exercise your rights under the GDPR, please see contact details below:

Data Protection Officer
Welsh Government
Cathays Park
CARDIFF
CF10 3NQ
Email: DataProtectionOfficer@gov.wales

If you are dissatisfied with the Welsh Government's handling of your request, you can ask for an internal review within 40 working days of the date of this response. Requests for an internal review should be addressed to the Welsh Government's Freedom of Information Officer at:
Information Rights Unit,
Welsh Government,
Cathays Park,
Cardiff,
CF10 3NQ

or Email: Freedom.ofinformation@gov.wales

Please remember to quote the ATISN reference number above.

You also have the right to complain to the Information Commissioner. The Information Commissioner can be contacted at:
Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,

SK9 5AF.

However, please note that the Commissioner will not normally investigate a complaint until it has been through our own internal review process

Yours sincerely,