GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW61 **Version Number: 3** **Date of next review:** January 2028

INFORMATION SECURITY POLICY

Policy Statement

Public Health Wales is a public body, with information processing as a fundamental part of its purpose and core processes. It is important, therefore that the organisation has a clear and relevant Information Security Policy.

Policy Commitment

The purpose of the information security policy is to protect the confidentiality, integrity and availability of all physical and electronic information assets owned and managed by Public Health Wales. This policy aims to ensure compliance with all relevant legal, regulatory and industry requirements, including, Network and Information Systems Regulations, Freedom of Information Act, Data Protection Act, General Protections Regulations and any other subsequent legislation of the same effect, and to safeguard the organisation from security threats and data breaches.

Chief Executive statement of commitment:

We are committed to preserving the confidentiality, integrity and availability of all data within our various systems. We recognise that we have a responsibility to protect all the data we hold or process, whether it is regarding our work, our staff, people who use our services, our research activities, the public, our partners or our suppliers. By protecting this data, we can ensure that we maintain our reputation as a trusted employer and source of information, enabling us to grow as an organisation and continue to deliver exceptional services.

It is the responsibility of all of us in Public Health Wales, to understand and acknowledge our security management processes and to comply with all information security policies and the procedures that underpin them.

We commit to ensure that our security management systems and processes are efficient, effective and continuously improving to protect our data assets.

Tracey Cooper – Chief Executive

Supporting Procedures and Written Control Documents

All corporate policies and procedures are available on the Public Health Wales website

Digital Assurance Procedure

Information Governance Policy

Internet Acceptable Use Policy

Email Acceptable Use Policy

Scope

This policy applies to:

- The workforce of Public Health Wales, including staff, Independent (Non-Executive) Board Members, students, trainees, secondees, volunteers, contracted third parties and any other persons undertaking duties on behalf of the organisation.
- All Information Assets, systems, networks, hardware, software, and data owned, managed or processed by Public Health Wales.

Equality and Health Impact Assessment	An Equality, Welsh Language and Health Impact Assessment has been completed and can be viewed on the policy webpages.
Approved by	Audit and Corporate Governance Committee
Approval Date	14/01/2025
Review Date	14/01/2028
Date of Publication:	22/04/2025
Group with authority to approve supporting procedures	Senior Leadership Team
Accountable Executive Director/Director	Iain Bell, Director of Research, Data and Digital and Senior Information Risk Owner
Author	Jonathan Jones, Lead Cyber Security Manager

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 the Board Business Unit.

This is a controlled document, the master copy is retained by the Board Business Unit .

Whilst this document may be printed, the electronic version posted on the internet is the master copy. Any printed copies of this document are not controlled. This document should not be saved onto local or network drives but should always be accessed from the internet.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**
3	2024	10/03/2025		Previous NHS Wales Policy now Superseded by PHW Information Security Policy
2	2021	20/07/2021		Adoption of AW17 NHS Wales Information Security Policy
1	2017	24/10/2017		First PHW version of Policy

1. Roles & Responsibilities

- **Chief Executive Officer**

The responsibility for information security resides with the Chief Executive Officer (CEO). This responsibility is discharged through the designated role of Senior Information Risk Owner (SIRO).

- **Data Protection Officer**

As a public authority Public Health Wales is required to appoint a Data Protection Officer (DPO) by the General Data

Protection Regulation (GDPR). The DPO is responsible for providing advice and guidance to the organisation on data protection requirements, monitors compliance with relevant data protection laws and policies and is the first point of contact for all data protection matters. The DPO reports to the Executive Director for Nursing, Quality and Integrated Governance (NQIG) but can act independently on data protection decisions.

- **Senior Information Risk Officer**

The Senior Information Risk Officer (SIRO) is responsible for ensuring that information security and information governance risks are managed, the SIRO advises the board on the effectiveness of information risk management across the organisation.

- **Caldicott Guardian**

A senior person with delegated responsibility from the CEO for protecting the confidentiality of patient and service-user information, and helping to ensure this information is used ethically, legally and appropriately.

- **Information Asset Owner**

The Information Asset Owner (IAO) is responsible for ensuring the protection, management and proper use of specific information assets under their control. The IAO is responsible and accountable for the information asset and will ensure legal and regulatory compliance in relation to the information asset storage and use.

- **Head of Digital Experience and Services**

The head of digital experience and services, supported by the digital leads, is responsible for supporting the implementation of controls within this policy, ensuring relevant staff are made aware of this policy and adhere to it and providing demonstrable support to the enablement of Information Security within PHW.

The head of digital services, supported by the digital leads, is responsible for ensuring all physical and electronic assets have adequate security

controls to comply with data protection and data security legislation and regulations.

- **Business & Service Owners**

Business and service owners are key staff who have responsibility for the delivery of services within PHW. Business & Service managers are responsible for the implementation of this policy within their department/ directorate.

- **Public Health Wales Workforce**

Managers are responsible for the implementation of this policy within their department/directorate. They must ensure that staff within their area of responsibility are aware of this policy, understand their responsibilities in complying with the policy requirements, and are up to date with the mandatory information governance and cyber security training module accessed via the NHS Electronic Staff Record. Where workforce members are not employees of PHW and they have a role that requires them to create, amend, access, or otherwise disseminate personal data or corporate information, processes must be in place to ensure they undertake regular suitable information governance training.

- **Cyber Security & IT Operations**

Cyber Security & IT Operations teams are responsible for developing, implementing, and enforcing suitable and appropriate information security procedures, controls and protocols to ensure Public Health Wales data, systems and networks remain compliant with relevant data protection legislation.

The Cyber Security team are responsible for the development and maintenance of this policy in line with organisational needs and Information Security best practice.

All workforce members must:

- Familiarise themselves with this policy and ensure its requirements are implemented and followed within their work area.
- Be aware that access to IT systems is monitored and audited.

Instances of non-compliance with this policy must be reported in accordance with local procedures.

2. Policy

The principal focus of information security is to provide the following:

- Confidentiality: The restriction of access to information by authorised persons, entities and processes at authorised times and in an authorised manner.
- Integrity: Safeguarding the accuracy and completeness of information and information processing systems.
- Availability: Ensuring that authorised users have access to information and associated assets when required.

2.1 User Controls

Access to information will be controlled on the basis of business requirements and the principal of least privilege (assigning the least number of privileges required for users to fulfil their work), all user requests for access to information and services will follow an approval process and require authorisation from the respective IAO or service owner.

All staff have the responsibility to only access the information which is required in order to carry out their duties. Examples of inappropriate access include but is not restricted to:

- Accessing your own health record
- Accessing any record of colleagues, family, friends, neighbours etc, even if you have consent, expect where this forms part of your legitimate duties.
- Accessing a record of any individual without a legitimate business requirement.

User access to is regularly monitored using National Intelligent Integrated Audit Solution (NIIAS) for all national systems. Inappropriate access can result in disciplinary action and in some cases criminal prosecution by the Information Commissioner or by the Director of Public Prosecutions.

If there are any concerns around the use or access of information, please express these to your reporting manager or the Information Governance Service.

2.2 Physical controls

All reasonable steps should be taken to ensure physical security of workspaces and physical assets. Badge and keycard access must be implemented where possible but always within restricted areas.

Restricted areas, such as server rooms, rooms hosting centralised networking and infrastructure equipment must be restricted to authorised staff only. These areas should also have CCTV deployed where possible.

Visitors should be "signed in" at authorised PHW work sites and always escorted in restricted areas.

Intrusion detection & alarm systems must be in place to detect unauthorised access and alert required staff.

Laptops and PC's must be protected by automated screen locks determine by a period of inactivity.

All mobile devices must be pin/ password protected and have automated screening locking in place.

Devices must not be left unattended in public workspaces, for example cafe's, train stations. Staff must lock devices when leaving the device unattended within authorised PHW work sites.

2.3 Environmental and Infrastructure controls

Restricted areas that host centralised networking and infrastructure equipment should have the following controls where appropriate:

- Climate control systems: Heating ventilation and Cooling systems must be implemented to protect servers and data storage systems from overheating.
- Uninterruptible Power Supplies (UPS): UPS' must be implemented to ensure availability of services during power outages and to prevent data loss.
- Fire Suppression Systems: Fire alarms and suppression systems must be in place to protect critical infrastructure assets.

2.4 Passwords

Public Health Wales workforce are responsible for the security of their own passwords, all passwords used must be strong and be hard-to-guess. Passwords must never be disclosed to anyone else.

Where the use of generic or shared accounts is required, passwords should be shared to the least number of authorised users and no further, when a member of staff with knowledge of shared accounts changes role or leave the organisation that account must have its password reset.

All default passwords for systems, services and infrastructure must be changed to a strong password.

Where staff have multiple accounts i.e. standard user, administrative, test – passwords must be not be re-used across different credential accounts.

Where possible and appropriate the use of Multi Factor Authentication/ Two Factor Authentication must be utilised. Multi Factor Authentication is mandatory for utilising Microsoft cloud resources.

PHW workforce must not logon to any computer system using another member's log in credentials without strict prior authorisation from Information Governance and the Head of Digital Experience and Services.

2.5 Remote working

Public Health Wales has a flexible approach to remote working and as such all-staff members are responsible for the security of their equipment and safeguarding of data.

Types of remote working (not exhaustive):

- Working from home
- Reading reports/ papers whilst travelling on public transport
- Working in public venues (e.g. coffee shops)
- Working whilst staying in hotels on Public Health Wales Business

Staff working remotely must utilise the corporate VPN to access resources.

All staff must be aware of their environment when working remotely, for example calls made/taken in less private space, visibility of your screen and the information displayed, all efforts must be made to ensure confidentiality.

If working in public spaces no equipment is to be left unattended, if staff stay at hotels whilst on PHW business all devices need to be secured, ideally in a locked safe.

2.6 Overseas working

There are instances where staff are required to travel overseas (outside the UK) to facilitate business on behalf of Public Health Wales, all staff must seek authorisation from the organisation and follow any relevant local organisational processes prior to travel.

Public Health Wales and DHCW (nationally) restrict and limit working overseas in specific countries due to risk and concerns of:

- Staff Safety
- Data Privacy concerns
- Local laws and regulations
- Cyber Security Threats

If working overseas is essential to a restricted/ limited country, approval must be granted by the SIRO.

2.7 Joiners, Movers, Leavers

A joiners (new starters), movers (employees changing roles or departments) and leavers (employees exiting the organisation) (JML) process is integral to information security, access to data and information systems must be managed throughout account life cycles.

To streamline the workforce members onboarding and offboarding process, it is required that line managers establish a standardised list of privileges (access rights) for each role within their department. This list should cover key areas such as network folder access, SharePoint pages, required software, Microsoft Teams groups and chats, and mailbox memberships.

This will help with:

- Improved efficiency – Accelerating new workforce member proficiency in their role.
- Preventing and identifying privilege creep – As line managers will know what permissions workforce members require, they can ensure that members do not acquire unnecessary elevated permissions as time goes by
- Removing permissions from internal movers – this will be easier to manage as line managers will immediately know what permissions they need to request be removed from the member's account

Joiners

All staff joining PHW will be granted access to required resources based on job role and in line with the principle of least privilege, access to any resource should be confirmed and approved by the employee's line manager.

IT Operations are responsible for the creation of Unique user computer log on ID's, mailboxes, assigning of any relevant equipment and enablement of multi-factor authentication.

All new starters must undergo formal induction and training within 3 months of starting their role.

Movers

When staff move job roles, it is the responsibility of the line manager to notify the relevant departments of the change, including IT Operations. IT Operations are responsible for reviewing and revoking access to user permissions where required, additional access to systems and services requires approval form the staff members line manager.

Leavers

When staff exit the organisation, it is the responsibility of the line manager to follow the PHW termination process as soon as reasonably possible after receiving the resignation notification, ensuring IT Operations are notified also. If staff are dismissed, any user account associated with the staff members must be immediately disabled and any active device users' sessions must be disconnected.

It is the responsibility of staff to return all equipment assigned to them on or before their last working day.

It is the responsibility of IT Operations to revoke all access to PHW systems and services, accounts should be disabled, and any shared user account passwords must be changed.

It is strongly advised that staff do not excessively share documents from their personal “OneDrive” accounts and they should also conduct regular user permission reviews, removing any unneeded access.

2.8 Supplier & Third party access

Any supplier or third-party access to PHW network or systems must be approved by IT Operations, where required national and local processes and procedures must be followed to attain the required assurance for any proposed access.

2.9 Storage & Ownership of information

All software, information and programmes developed for NHS Wales organisations by the workforce during the course of their employment will remain the property of the organisation.

Users are not permitted to use their personal devices, store confidential information on a personal device or unapproved 3rd party file storage services for the purpose of carrying out PHW business unless they have been explicitly authorised to do so in line with a documented organisational process (e.g. a Data Protection Impact Assessment).

Staff must not store information on local drives (usually referred to as the C Drive). Exceptions to this may be for legitimate work purpose to a device that is encrypted.

2.10 Information Sharing & Publishing

PHW are committed to safeguarding the confidentiality, integrity and availability of all information assets during the process of information gathering, handling and publishing, all staff are required to comply to data protection and data privacy laws and regulations.

Information is only gathered where required for business use, with special consideration of information sensitivity and intended use. Access to collected information is restricted to authorised staff only and has strong controls in place to prevent unauthorised access.

Information is to be stored, processed and transferred using encryption to prevent unauthorised access and data breaches. Information must be protected by strong access controls, retention policies and should be regularly audited to ensure security and accuracy of information.

Before publication a thorough review process must be in place to help identify, prevent or mitigate potential risks, including inadvertent release of sensitive information. Information publishing platforms must be secured through strong access controls, multi-factor authentication and real-time monitoring.

Information published should continue to be monitored for integrity and compliance.

Information is only to be shared with approved stakeholders, approval must be sought via Information Governance procedures and any sharing of information must be done securely.

2.11 Removeable media & Portable Storage

Whilst it is recognised that both portable devices and removable media are widely used throughout PHW, unless they are used appropriately, they pose a security risk to the organisation.

Removable media includes, but is not limited to, USB 'sticks' (memory sticks), memory cards, and external hard drives. Appropriate controls must be in place to ensure any information copied to removable media is secure.

Portable devices include, but are not limited to, laptops, tablets, Dictaphones®, mobile phones, cameras, and some forms of medical devices.

All portable devices must utilise appropriate technical measures to ensure the security of all data. Mobile devices and tablets must be managed using the PHW mobile device management solution.

Only approved and organisation provided devices are to be used for the transfer or storage of information, unless otherwise agreed by Information Governance and IT Operations.

All devices should be physically secure when not in use, and devices should not be left unattended.

2.12 Secure disposal

For the purposes of this policy, confidential waste is any paper, electronic or other waste of any other format which contains personal data or business sensitive information.

Paper

- All confidential paper waste must be stored securely and disposed of in a timely manner in the designated confidential waste bins or bags; or shredded on site as appropriate. This must be carried out in line with local retention and destruction arrangements.

Electronic

- Any IT equipment or other electronic waste must be disposed of securely in accordance with local disposal arrangements. For further information, please contact IT Operations.

Other Items

- Any other items containing confidential information which cannot be classed as paper or electronic records e.g. film x-rays, orthodontic casts, carbon fax/printer rolls etc, must be destroyed under special conditions. For further information, please contact IT Operations.

2.13 Security of assets

PHW will maintain a full inventory of major assets associated with its information systems. Asset will include:

- Physical Devices
- Software Applications
- Data
- Back-ups
- Software applications

The IT Operations team will monitor all systems and PCs to ensure that all propriety software products installed and utilised within PHW are used legal, are licensed and are part of the inventory management processes.

No software product should be used without the relevant and appropriate license and no product installation should exceed the number of licenses held by PHW.

Copying of propriety organisational software, for use on unmanaged or personal devices is prohibited for anything other than authorised organisational business.

Only software licensed and approved by PHW IT Operations is to be used on PHW devices, unapproved software can be removed without prior notice if identified.

Free software or academia software that requires to be installed on PHW devices must be approved by IT Operations prior to use.

Software installed must be free of vulnerabilities, security misconfigurations and must have regular managed software and security updates provided in a timely fashion, where software fails to meet any of these principals, IT Operations reserves the right to remove the software installation from any and all devices.

2.14 Anti-Virus Protection

Anti-virus protection is integral to ensure all systems and devices within PHW are protected against malware, viruses and other malicious software that can compromise the confidentiality, integrity or availability of organisation data and systems.

The follow statements apply:

- All organisational owned and managed devices must have anti-virus software installed, configured and maintained
- Anti-virus software must have automatic updates to virus definition database
- Regular anti-virus scans must be run regularly, this includes on demand and full systems scans – frequency to be configured by IT Operations
- Anti-virus software must have automatic updates and patches applied, any system found with outdated antivirus definitions or software versions may be restricted from the network
- Users must not disable, alter or remove any anti-virus software or other security applications from PHW owned and managed devices
- Users must not install any additional anti-virus software to PHW devices
- Users must report any suspected or detected malware to IT Operations immediately
- Only IT Operations are permitted to make changes to anti-virus configurations or installations.
- IT Operations reserve the right to isolate, manually or automatically, devices from the network where malware is identified or deemed a threat to organisation information systems or data.

2.15 Back-up and recovery

All critical systems, data and applications owned, managed and supported by PHW will be backed up as part of the organisational backup programme, it is the responsibility of the IAO's to ensure the back-up requirements align with individual service and overarching business needs.

Back-up data must be securely stored and only accessible by authorised individuals.

A back-up plan must be held for all services owned and managed by PHW.

Unless specifically agreed with IT Operations any information held on local hard drives, portable devices or removable media will not form part of the PHW backup programme.

IT Operations are responsible for the back-up and storage of required and relevant encryption keys related to the back-up procedure(s).

Back-ups should be validated for integrity and where failures are identified, these are to be communicated to the Head of Digital Experience and Services, investigated for resolution and additional back-ups are to be taken at the earliest opportunity.

Back-ups of systems deemed critical to the function of PHW operations must be copied and stored in the immutable back-up solution. Immutable back-ups (that cannot be altered / tampered with) must also be validated for integrity.

Systems, services and core components must have scheduled recovery exercises undertaken, at least bi-annually. Any identified issues or improvements must be amended to the service/ system back-up and recovery plan(s).

2.16 Business Continuity and Disaster Recovery

Business Impact Analysis' must be undertaken by Business & Service owners for each system in use within PHW to ascertain the level of criticality and to be compliant with the Network and Information Systems (NIS) Regulations.

Business continuity and disaster recovery plans must be developed, documented and maintained for all systems & services owned and managed by PHW. The plans must identify critical operations and outline recovery time objectives and recovery point objectives.

Business continuity and disaster recovery plans must cover all essential business functions.

It is the responsibility of Business & Service owners to ensure that Business continuity and disaster recovery plans are documented, readily accessible and regularly reviewed and updated in line with service and organisational needs.

Business continuity and disaster recovery plans must be tested regularly, through simulations, tabletop exercises or live drills to ensure accuracy effectiveness and that staff are fully aware of their roles in an emergency.

All plans must be reviewed and updated following significant organisational change, incidents or as result of testing.

2.17 Incident Response

Incident response is essential to ensure the readiness of PHW to manage security incidents effectively, safeguard data and maintain compliance with laws and regulations.

All suspected security incidents, including data breaches, malware infections must be reported to cyber security immediately as detailed within the local PHW Cyber incident response process and subsequently logged on the incident management platform.

It is the responsibility of the Cyber security team to ensure that a Cyber Incident response plan is documented, reviewed and updated regularly, and that decision logs for incidents are completed and stored securely.

2.18 Digital Assurance

Assurance must be sought and maintained for all digital assets within PHW, including software applications, IT infrastructure, data, cloud services and third-party products and services.

It is the responsibility of all staff to ensure the relevant PHW procedure(s) are followed prior to any changes being made to digital assets or services going live.

Risk Management and Assessment

- Risk assessments must be conducted on all digital assets to identify, prioritise and remediate potential security risks and vulnerabilities.
- Risk remediation and mitigations must be implemented for identified risks, any exceptions must be logged on the risk management platform.
- Monitoring must be in place to identify threats and vulnerabilities for digital assets.

Secure Development

- Systems should be secure by design; security principles and best practice must be embedded into all stages of software development.
- Regular security testing programmes must be in place for information systems.
- All systems and services must be security tested prior to go-live and any identified risks are to be addressed.

Third-Party Assurance

- Any use of third-party supplied applications, services or environments must be assessed and approved prior to use.

- Third-party suppliers must adhere to relevant laws and regulations and meet any internal security standard and requirements.

- Third-party contracts must include clearly defined security requirements and responsibilities as required by PHW.

2.19 Training & Awareness

Information security and information governance is the responsibility of all of the PHW workforce. Training for Cyber security and information governance is mandatory for all PHW staff and must be completed at least every 2 years.

The workforce should be aware of the legal, professional and ethical obligations that apply to them when accessing information systems and information assets, where this is unclear please contact the Information Governance Service.

2.20 Monitoring & Compliance

PHW reserves the rights to monitor and audit business activities and processes for all networks, systems and digital assets to ensure the effectiveness of services, comply with relevant laws and regulations and adherence to this policy.

A considered approach is taken to all monitoring tools or processes used with PHW and great emphasis is placed on the privacy of employee's data and activity. Any data collected will be relevant and legitimate to the needs of the business, it will be stored securely and accessed only by authorised personnel when required.

3. References – Legislation

The Data Protection Act (2018)
The UK General Data Protection Regulation
The Copyright, Designs and Patents Act (1988)
The Computer Misuse Act (1990)
Network and Information Systems Regulations (2018)