GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** xxxx **Version Number:** xxx **Date of next review:** xxx

INFORMATION GOVERNANCE POLICY

1. Policy Statement

This Policy has been developed by Public Health Wales and is adapted from the national Information Governance Policy

The policy consolidates and replaces the following national policies:

- NHS Wales Information Governance Policy
- NHS Wales Information Security Policy
- NHS Wales Internet Use Policy
- NHS Wales Email Use Policy

2. Policy Commitment

The purpose of this policy is to provide staff (see section 3, 'scope', below) with a framework to ensure that all information is acquired, stored, processed, shared and transferred, safely and securely in accordance with the law and associated standards.

The objectives of the policy are to:

- Set out legal, regulatory, and professional requirements;
- Provide staff with the necessary principles to understand and fulfil their responsibilities in ensuring the confidentiality, integrity, and security of information.

3. Scope

This policy applies to all PHW staff, including Independent (Non-Executive) Board Members, employees, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of PHW whether in temporary or permanent posts and the use of the term 'staff' in this Policy should be read to mean the above.

This policy applies to all forms of information processed by or on behalf of PHW regardless of format, including but not limited to paper or electronic records.

4. Roles and responsibilities

The Chief Executive Officer (CEO) is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation. PHW must have in place appropriate local information governance management arrangements.

To ensure the ability to comply with data protection legislation, PHW has in place the following role:

- **Data Protection Officer (DPO):** An independent data protection expert who is responsible for monitoring an organisation's compliance; informing and advising the organisation on its data protection obligations and acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

PHW has also appointed the following key roles:

- **Senior Information Risk Owner (SIRO):** An Executive Director or member of the Senior Management Board of an organisation with delegated responsibility from the CEO for the organisation's information risk policy. The SIRO is accountable and responsible for information risk 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;

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 staff 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.

Staff must familiarise themselves with this policy and ensure its requirements are implemented and followed within their work area. Instances of non-compliance with this policy must be reported in accordance with local procedures.

5. Policy

5.1 Principles

All staff are legally accountable for organisational assets and must ensure that information is processed in line with the data protection legislation.

5.2 Standards

This policy aims to assist in maintaining the following four key standards:

- **Openness:** PHW will support the principles of openness and transparency and welcomes the right of access to information provided by relevant legislation.
- **Legal Compliance:** PHW will comply with relevant legislation, and the common law, relating to the management and use of information.
- **Information Security:** PHW will establish and maintain policies for the effective and secure management and operation of all information assets regardless of whether these are in paper form or stored within its digital network.
- **Information Quality Assurance:** PHW will promote information quality and effective records management through the provision of relevant policies, procedures, guidance, and training.

5.3 Data Protection Impact Assessments (DPIA)

A DPIA must be undertaken by law where any processing is likely to result in a high risk to the rights and freedoms of individuals or in any case where there is to be:

- A systematic and extensive profiling with significant effects.
- Large scale use of special categories of data or of personal data relating to criminal convictions and offences.
- Public monitoring.

For the purpose of this policy, processing may be high risk where the processing:

- Involves the use of innovative technologies, or the novel application of existing technologies, including artificial intelligence.
- Relates to an automated decision-making process that influences whether an individual or group of individuals can access a product, service, opportunity or benefit based on profiling or involves the use of special category data.
- Consists of any profiling of individuals on a large scale.
- Is of that of biometric data.
- Is of genetic data except for the provision of direct care by a healthcare professional.
- Where data is combined, compared or matched with other personal data obtained from multiple sources.
- Where data has not been obtained directly from the data subject and the use of the data means that contacting data subjects to advise of the processing would prove impossible or involve disproportionate effort.
- Involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
- Relates to children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if online services are to be offered directly to children.
- Is of such a nature that a personal data breach could jeopardise the health or safety of individuals.

Staff must consider whether a DPIA is required and seek the advice and guidance of the relevant organisation's Information Governance department or team at the beginning of any project and prior to the processing of any personal data.

5.4 Third Parties and Contractual Arrangements

Whenever PHW engages a data processor or any other form of supplier that involves the collection, storage, processing, analysis, use and dissemination of personal data, there must be a written contract or other legal instrument in place that clarifies responsibilities and liabilities for information and data. Agreements between PHW and any processors must provide that no sub processor should be appointed without prior authorisation.

Where the processor utilises a sub processor, PHW must be satisfied that the sub processor has an equivalent level of protection for the personal data as those in the contract between PHW and the processor before authorising that sub processor.

A proposed transfer of personal data outside of the UK is referred to as a 'restricted transfer'. In such circumstances individual rights around personal data must be protected or one of a limited number of exceptions must apply in order for the transfer to proceed. PHW must assess and apply such protections as specified in legislation and ICO guidance to such transfers. Staff must contact the Information Governance Service to seek advice and guidance before such transfers are made.

5.5 Information Sharing

PHW must put in place formal agreements when sharing information with other organisations. Such agreements provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information. Advice must be sought from the Information Governance Service in such circumstances.

The Wales Accord on the Sharing of Personal Information (WASPI) framework is in place to assist organisations to share personal data effectively and lawfully. Where a NHS Wales organisation is a signatory to the Accord it must use WASPI templates where they are relevant to the proposed sharing. Further advice is available on the WASPI website: www.waspi.gov.wales.

Where there is a requirement for sharing information due to safeguarding concerns, there should be a presumption towards the sharing of the necessary information with the appropriate parties in line with appropriate policies.

5.6 Sharing Personal Data in an Emergency

In an emergency situation (e.g. where there is a serious threat to life or safety) personal data may be shared without a formal agreement. The sharing of such information must be formally documented, evidencing why the information needed to be shared. In these circumstances the decision can be documented retrospectively. Staff should exercise their professional judgement in such circumstances. PHW will support staff to make appropriate decisions by providing support, guidance and training.

5.7 Inappropriate Use of the NHS Wales Network

Inappropriate use of NHS Wales IT services is prohibited. For the avoidance of doubt, the appendix to this policy sets out what is considered to be inappropriate use.

Staff must not use NHS Wales IT systems in any way to access, create, transmit or store material (including on Non-Corporate Communication Channels (NCCC)) that is likely to bring PHW into disrepute or incur liability on the part of PHW. Where a job requires a member of staff to send, receive, or access material that could be considered offensive, arrangements must be authorised to facilitate this requirement.

To avoid any inadvertent breaches of this policy, PHW will block any communications and internet sites containing prohibited content by default. Procedures are in place to consider applications for exceptions.

Local restrictions within PHW ensure that only individuals employed by, or on behalf of, PHW with a genuine business need are given access to manage social media accounts for business use. Staff must also comply with the NHS Wales Social Media Policy when using social media.

Anyone using social media on behalf of PHW has a responsibility to conduct themselves in an appropriate manner, as they should when addressing the media or any public meeting or forum.

Users must ensure that IT facilities are used appropriately at all times.

At no time should the NHS Wales IT network be used for any activity by which an individual makes a personal financial gain, including selling goods or services.

5.8 Communications using NHS Wales IT resources

Staff must be aware of the risk of sending any communications messages. This includes using tools such as email and instant messaging and using any functionality within shared internal or external resources whereby information or messages can be communicated. The risk will be higher where the information being communicated relates to identifiable individuals (personal data), particularly where the subject matter is confidential or includes Special Categories of personal data as set out in data protection legislation.

Security measures appropriate to the level of risk must be employed in all circumstances, with particular caution applied when data is sent outside of the NHS Wales IT network. When sending any communication users must be vigilant and ensure that contact details (including email addresses) are up to date and correct. Tools such as the Secure File Sharing Portal must be used where appropriate.

Limited personal use of PHW communications systems is permitted and in the case of email this is covered by the Email Acceptable Use Policy.

Staff must not subscribe to third party services unless they are part of a recognised scheme for the employer (e.g. health and wellbeing schemes promoted by the employer). For the purpose of this policy, the following uses are considered to be consistent with work purposes:

- Communications sent to occupational health.
- Communications connected to Health and Wellbeing incentives.
- Communications connected with approved personal development / training.
- Communications with Trade Unions and Professional Bodies.
- Communications in an emergency situation.

5.9 Access Management

Access to information must be based on an individual's role.

Taking into account the capabilities of applications and IT systems, the minimum level of access required for staff to undertake duties associated with their employment should be provided. Staff must only access information required to undertake duties associated with their employment. Access to any information, including information about themselves or any other individual, is prohibited unless it is required as part of their role and does not constitute a conflict of interest.

All staff are responsible for ensuring that the security of information is maintained regardless of the setting (for example, when working from home or working in the community).

Where file servers exist, access must be restricted to those designated members of staff that require access as part of their role (typically system administrators, data architects and similar roles). Staff must not access or attempt to access this equipment unless it is a part of their role.

Passwords for individual accounts must not be disclosed, and users of IT systems must not under any circumstances allow their accounts to be used by others.

Where shared accounts exist to access any historic IT infrastructure or to log on to the network using dedicated IT equipment, usernames and passwords should be changed regularly and not shared beyond the team responsible for operating those services. Any local or national systems and services

accessed via these computers must only be done so using individual usernames and passwords to enable audit of services.

Leavers and movers procedures must be followed when a member of staff either leaves their current role for another in a different department, or leaves the organisation. This ensures that access to systems and buildings is managed appropriately, and that security is not compromised. Confidential information, including access rights to confidential information on systems, must not be transferred to a new role if not required for that role.

Any suspected breach of security must be reported as soon as possible in accordance with local procedures in force within PHW.

5.10 Personal Devices

Staff are not permitted to use their personal device to access or attempt to access the NHS Wales internal network that exists behind password protected security controls, unless accessed via the software made available by PHW.

Staff must not store or attempt to store confidential information on personal devices unless this is stored using software made available by the NHS in Wales for that purpose.

By default, photographs must not be taken of individuals in any patient areas of NHS premises using a personal device. In areas designated as 'staff only' that are not accessed by patients, a personal device must not be used to take any photograph unless approved by the appropriate head of service following a risk assessment to ensure that the confidentiality of individuals in those images and the security of any organisational measures that may be in place. It must also be remembered that this applies to staff as well as service users.

5.11 Backup

Where it is proposed that any information is to be stored in a location not connected to the NHS network, a risk assessment must be undertaken and reviewed by the SIRO or another individual with delegated authority to make decisions. In all circumstances, information must be uploaded to the relevant filing structure, to include shared drives, clinical systems, records management systems, or SharePoint sites as soon as is reasonably practical given the circumstances. Organisational procedures or other guidance must be in place to ensure staff are aware of their responsibilities.

5.12 Disposal of confidential information and computer hardware

Confidential information in paper format, and any IT equipment that is capable of storing information must be disposed of using accredited secure waste disposal companies. Organisational leads procuring such services must ensure that these companies comply to the relevant security standards. An appropriate contract must be in place to ensure that roles and responsibilities are clear and liability in the event of data breach is clear.

5.13 Records Management of Communications

Staff should be aware that it may be necessary to conduct a search and disclose information in response to information requests, to conduct an investigation or as part of a Public Inquiry, and that this may take place with or without their knowledge or consent.

Communication tools (for example, Outlook and Teams chat messages) must not be used as a long-term storage facility. Emails / messages that need to be retained must be saved securely to the appropriate record (e.g. to a clinical / business record or appropriate Sharepoint location)).

Retention policies must be set as appropriate in accordance with the current issue of the NHS Wales Records Management Code of Practice for Health and Social Care.

5.14 Intellectual property

Intellectual property created by PHW remains the property of that organisation. Unpublished documents created by staff must not be published or made available to any individual not employed by PHW outside of normal organisational arrangements, such as Publication Schemes created under the Freedom of Information Act 2000, or in response to a request for information in line with the law and approved processes.

All software, information, and programmes developed for PHW by staff during the course of their employment will remain the property of the organisation. For more information staff should consult the Intellectual Property Rights Policy

5.15 Information Asset Management

The processing of information assets will be catalogued and managed by PHW, using an Information Asset Register which must be regularly reviewed and updated and contribute to the organisation's Record of Processing Activity (ROPA).

The Wales Control Standard for Electronic Health and Care Records describes the principles and common standards that apply to shared electronic health and care records in Wales. A register of core national systems is maintained by Digital Health and Care Wales.

5.16 Incident and risk management

PHW has policies and procedures in place to:

- Identify and manage risks to the confidentiality, integrity and availability of data and information for which they are responsible.
- Report, manage and resolve any breaches under this policy.
- Identify and implement lessons learned.

Information Asset Owners are responsible for determining the appropriateness of any security measures required to protect information assets based on local risk assessments, including Data Protection Impact Assessments.

Incidents must be reported promptly and in any case in line with current legislation.

5.17 Training and Awareness

Information Governance, Records Management and Cyber Security Training is mandatory for all staff and must be completed at commencement of employment and at least every two years. Non

NHS employees must have appropriate Information Governance training in line with the requirements of their role.

5.18 Monitoring and compliance

PHW reserves the right to monitor and audit activity in business premises, use of business facilities, and the working practices of its employees to ensure compliance with this policy, compliance with legislative requirements, and the effectiveness of the services provided. This will include monitoring and auditing equipment such as CCTV systems, access control entry systems, and any IT equipment used in the service.

When any monitoring of employee activities, PHW assesses:

- The purpose of the auditing and what it intends to achieve
- Whether the information to be collected through monitoring is necessary to fulfil the purpose of the monitoring, ensuring always that the business interests the monitoring seeks to protect are legitimate.
- Whether the appropriate balance of the privacy of employees has been considered.

Monitoring tools must be used according to an assessed purpose only, and the data from any monitoring or audit must be kept secure.

Impact Assessments	This policy has been subject to an equality assessment. The assessment determined that this policy was not discriminatory or detrimental in any way with regard to the protected characteristics, the Welsh Language or carers.
Approved by	
Approval Date	
Review Date	
Date of Publication:	
Group with authority to approve supporting procedures	Senior Leadership Team
Accountable Executive Director/Director	Iain Bell, National Director of Public Health Knowledge and Research and Senior Information Risk Owner
Author	John Lawson, Head of the Information Governance Service

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**

Appendix 1

Inappropriate Use

For the avoidance of doubt, PHW consider any of the following to be inappropriate use:

- Knowingly accessing NHS Wales IT services of another PHW employee with or without their knowledge (for example, using someone else's username and password). This excludes sending a communication as an authorised delegate of that member of staff (for example, an executive assistant sending a communication on behalf of a senior manager, where those delegated responsibilities have been agreed)
- Allowing access to any NHS Wales IT services to someone not authorised to access those services (for example, allowing a friend, family member use a NHS Wales/PHW laptop or access resources via a personal device).
- Uploading, communicating, or otherwise disclosing confidential information in any way without authorisation, or without the appropriate security measures being in place.

- Knowingly downloading, viewing, communicating or saving, or attempting to download, view, communicate or save any information or images which are unlawful or could be considered to be:

  Defamatory
  Offensive
  Abusive
  Obscene
  Hateful
  Pornographic
  Indecent
  Displaying, promoting or describing acts of violence
  Displaying, promoting or describing acts of terrorism
  Discriminatory
  Bullying or harassing to any person.

- Intentionally publishing or communicating false information about NHS Wales organisations or NHS Wales staff, clients or patients.
- Knowingly breaching copyright or Intellectual Property Rights (IPR).
- Hacking into others user accounts, or using the NHS Wales network to hack into other accounts.
- Downloading, installing, sending or otherwise distributing unlicensed, illegal or unauthorised software.
- Deliberately attempting to circumvent security systems protecting the integrity of the NHS Wales network.
- Deliberately disabling or overloading any ICT system or networks, or attempting to disable or circumvent any system intended to protect the privacy or security of employees, patients or others;
- Altering any of the system settings on NHS Wales owned IT equipment or trying to change the access server to avoid, or attempt to avoid, restrictions imposed by the filtering software.
- Intentionally introducing malicious software such as Viruses, Worms, and Trojans into the NHS Wales network.
- Knowingly and without authority viewing, uploading, or downloading material that may bring PHW into disrepute; or material that could cause offence to others.
- Distributing unsolicited commercial or advertising materials.
- Using IT equipment supplied or paid for by PHW with the intention of making a personal gain (for example - running a business).
- 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.
- Forwarding chain messages or spam (unsolicited messages) within PHW or to other individuals or organisations.
- Excessive personal use or personal use outside of that described in this policy or local policies and procedures.