Cardiff and Vale UHB
Information Governance Policy

Author: Information Governance Department
Approved by: Information Governance Executive Team
Approved by: Digital Health Intelligence Committee
Version: 0.4
Date: 20/02/2026
Review date: 2 years following ratification

Contents

1. Introduction

Cardiff and Vale UHB considers information to be a vital asset, and a key enabler, on which the UHB is dependent as we move forward in delivering our Shaping Our Future Wellbeing strategy and becoming a data driven organisation.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

2. Purpose

It is the policy of the UHB to ensure that:

- We protect the legal rights of individuals, patients and staff in respect of confidentiality and privacy.
- We safeguard our information and systems.
- We make appropriate use of ICT services, such as email and the internet.
- Our staff have access to the relevant and appropriate information they require at the point that it is required.
- The value of the information that the UHB manages is increasingly realised
- All services transition towards the appropriate adoption of the UHB's technical and data standards and achieve these by 2023.
- Opportunities to achieve improvements in clinical and cost-effective care provided by digital technologies are realised.
- We improve the ability of our population, patients, and staff to make timely, evidence-based decisions.
- Our staff are valued, trusted and enabled.
- Our staff are supported to better manage and balance work and out-of-work commitments.
- We comply and act in the intended spirit of the Welsh Government's policy and notably the 'Once for Wales' design principles.

3. Scope

This policy applies to the workforce of Cardiff and Vale UHB including staff, students, trainees, secondees, volunteers, contracted third parties and any other persons undertaking duties on behalf of the UHB, across all areas of our business, including: the provision, planning and commissioning of direct care, teaching and training; and scientific work including research.

It applies to all forms of information controlled and processed by Cardiff and Vale UHB including video, digital and paper; and covers all business functions and the information, information systems, networks, physical environment and relevant people who support those business functions.

The policy covers the following areas:

- Roles and Responsibilities
- Use and protection of Data

- Data and technical standards
- Privacy notices
- Information security
- Internet Use
- Email Use

4. Roles and responsibilities

This policy is intended to be enabling and expects that the professionalism of all staff to familiarise themselves with the policy content and ensure the policy requirements are implemented and followed at all times. In adopting a high trust approach, it is an absolute requirement that all staff members undertake the appropriate level of information governance training at least every two years. It is also essential that breaches of this policy and related legislation are reported by the individual via Datix or agreed local reporting mechanisms and to the Data Protection Officer at the earliest opportunity.

UHB.DPO@Wales.NHS.UK

The UHB's accountability and governance structure for Information Governance requires specific roles to be fulfilled. These are set out below:

The Chief Executive is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation and any associated legal requirements. The Chief Executive is responsible for ensuring that there is a designated individual within the UHB who assumes the responsibilities of three statutory positions.

The Data Protection Officer is responsible for to ensuring that the UHB processes the personal data of its staff, patients and population in compliance with the data protection legislation.

The Senior Information Risk Officer (SIRO) is responsible for ensuring that information security and information governance risks are managed. Specific responsibilities include:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers.
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently by Information Asset Owners.
- Advising the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal controls.
- Owning the organisation's information incident management framework.

The Caldicott Guardian is responsible for safeguarding the processing of patient information.

The Head of each Clinical Directorate, Clinical Board & Corporate Department is responsible for appointing Information Asset Owners and Administrators to act as accountable officers and named points of contact for IG matters.

Information Asset Owners are responsible for the implementation of this policy in respect of the data held acquired, stored within their assets and transferred from their assets (e.g. IT systems, databases, video stores, clinical record libraries). Specifically, Information Asset Owners should have undertaken a self assessment of their directorate's compliance with data protection regulation, using the ICO's tools (link: https://ico.org.uk/for-organisations/data-protection-self-assessment/) once every 24 months and have logged completion with the IG department. Information Asset Administrators will support the Information Asset Owners in fulfilling these obligations.

Managers are responsible for the implementation of this policy within their department/directorate. In addition, they must ensure that their users and staff are aware of this policy, understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training.

5. Data Protection and Compliance

Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared.

While the emphasis on this policy is on the protection of personal data, the UHB owns and processes business and other sensitive data. The security of 'sensitive' data is also governed by this policy.

5.1.1 Definition of Personal Data

For the purpose of this policy, the use of the term "personal data" encompasses any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Personal data that has been pseudonymised – e.g. key-coded – will fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

5.1.2 Special Categories of Personal Data

Special categories of personal data are defined by data protection legislation as including any data concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic and biometric data where processed to uniquely identify an individual.

5.1.3 Data controller and data processor

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the

purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

5.1.4 Anonymisation and pseudonymisation

Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

5.2 Using data

5.2.1 Fair and Lawful Processing

The UHB will process personal, special category and sensitive data fairly and lawfully, in line with data protection legislation and in accordance with the UHB's patient and staff privacy notices. Processing broadly means collecting, using, disclosing, sharing, retaining or disposing of personal data or information.

In order for the processing of data to be fair, the SIRO, on behalf of the UHB will maintain and publish in a highly open, transparent and accessible way, privacy notices for patients and staff which clearly set out the information held by the UHB and how it is used are available below.

Patient Privacy Notice

Employee Privacy Notice

All sizeable patient facing areas should provide patients with clear information signposting them to the web page at which the UHB's privacy notice for patients can be viewed. It is the responsibility of the manager of the clinical area to have this in place.

Where an activity can be carried out without the need for personal or sensitive data to be disclosed, anonymised data should be used. Where personal data is required, then the minimum amount of identifiable information required should be used and, wherever appropriate, the data should be pseudonymised.

Personal or sensitive information should not be processed where the UHB does not have a lawful basis for processing such information under the data protection legislation which is not reliant on the consent of individuals (e.g. necessary for the health or social care purposes). Exceptions to this must be agreed with the SIRO and Caldicott Guardian.

Where there are any queries, staff must consult the Information Governance Office before processing or sharing personal or sensitive data.

5.2.2 Information Asset Management

5.2.1.1 Information Asset Registers

To protect individual's rights laid out in the Data Protection Act 2018 and the UK GDPR (2018), it is important that the UHB has knowledge of, and can swiftly access, all of the personal and sensitive data that it holds, regardless of the medium in which it is held. To achieve this, each Clinical Directorate, Clinical Board and Corporate Department must identify and record the lawful basis for the information it processes in an information asset register. It is the responsibility of the Information Asset Owners to ensure that the information asset registers are accurate and up to date and the responsibility of individual members of staff to store data they hold in a way it can be accessed swiftly.

As a minimum, information asset registers should document all "departmental" shared drives managed by an individual within the Directorate, all servers owned by the directorate and all systems used and contracted for by the Directorate (including messaging systems), incorporating:

- the type of information held
- where it came from,
- who it is shared with
- how this information is used
- the legal basis for holding this data – If in doubt consult the UHB's web page or ask the IG department
- When it should be destroyed (if not in the medical record or essential for business use – e.g. a contract, then the longest retention period including email should be 6 months unless specifically referenced in the UHB's retention schedule, available via Information Governance webpage.
- Who this data is shared with – e.g. Royal Colleges, WG, other NHS organisations, Local Authorities
- Where data is shared, the legal basis for sharing the data (as above, public duty should be used where the basis is patient care)
- Confirmation that no data is stored or transferred outside the European Economic Area, including for Artificial Intelligence processing within the cloud.

5.2.1.2 Registering Security, Hosting and Back up arrangements

To ensure that the UHB maintains service resilience in line with the EU directive on the security of Networks and Information Systems, all existing and new systems provided or used by the UHB should have a Security, Hosting and Back Up agreement with the UHB's informatics department, with the required details included on the information asset register. It is the responsibility of the Information Asset Owners to ensure that these details are accurate and up to date.

5.2.1.3 Managing paper care records

Members of staff who have received and are using the paper care record are responsible for ensuring that the location of the record is known and tracked on the appropriate electronic system.

The paper care record must not be split. Where only a single volume of a file containing several volumes is required, this may be moved for a very minimal time (never longer than the current working shift) and holders of both segments of the record must be aware. This must be reflected via the tracking mechanism on the appropriate electronic system.

5.2.1.4 Storing and moving data

Section 6.1 refers to expected standards and requirements for the control and storage of data.

5.2.3 Individual's Rights & Consent

Individuals have certain rights with regard to the processing of their personal data. Information Asset Owners must ensure that appropriate arrangements are in place to manage these rights.

In particular, where the directorate is reliant on "Consent" as the legal basis for holding patient identifiable data, you must ensure that the way you have attained the consent follows the ICO's guidance:

- A request to gain consent to use information about the patient should be made prominent and be clearly separated from other requests for consent – such as those in regards to treatment.
- Consent has required a positive opt-in such as un-ticked opt-in boxes or similar active opt-in methods.
- Consent should be specific and granular. You should allow individuals to consent separately to different purposes and types of processing wherever appropriate.
- Be clear that this consent is for NHS Wales & Cardiff and Vale UHB and name any specific third party organisations that will rely on this consent.

5.2.4 Accuracy of Personal Data

Arrangements must be in place to ensure that any personal data held by the UHB is accurate and up to date, or contains a time stamp.

5.2.5 Establishing new data processing activities

New data processing activities include, but are not limited to: the introduction of new data capture systems, the collection of additional data items, the undertaking of Artificial Intelligence which does not involve the intervention of a human and extending the sharing of data.

5.2.5.1 Data Protection Impact Assessment (DPIA)

All new projects or major new flows of information must consider information governance practices from the outset to ensure that personal data is protected at all times. Any processing that is likely to result in a high risk must be assessed by a DPIA, especially any transfer outside of the European Economic Area. This also provides assurance that the UHB is working to the necessary standards and are complying

with data protection legislation. In order to identify information risks, a DPIA must be completed. If there is any doubt as to what and whether a DPIA is required, the information governance department should be requested to assist.

The results of the DPIA must both be filed and discussed with the Information Governance Department (who may consult the ICO) and signed off by the UHB's Data Protection Officer and Senior Information Risk Owner. Any controls identified as being required must be acted upon and put in place.

5.2.5.2 Third Parties and Contractual Arrangements

Where the organisation uses any third party who processes personal data on its behalf, any processing must be subject to a legally binding written contract which meets the requirements of data protection legislation.

UHB documents & specifications (such as the UHB's Data Processing Contract, Security Arrangements, Contracts, Procurement technical specification, codes of conduct, access and auditing specifications) must be used in formalising the arrangements for the processing and sharing of the personal data the UHB controls or will be controllers of (that which it processes for its own purposes). This is to ensure that personal data is processed in a consistent manner and the roles of responsibilities of the parties are clearly understood.

No part of a UHB agreement can be varied without the prior written approval of the relevant Director, particularly the minimum indemnity limit of £5 million per annum.

5.2.5.3 Documents and forms used to collect personal data

All forms (both computerised and manual) used to obtain personal data must comply with the requirements of DPA. Personal information must be adequate, relevant and not excessive, and specifically no unnecessary information to be included.

Forms will be reviewed by the author and/or responsible manager and then sent to the Information Governance Department for sign off and will be periodically audited to ensure that the personal data being processes complies with the DPA.

The IG Department will be responsible for providing advice and guidance regarding compliance with 'Adequate Data'. Legal advice will be sought for any unclear or contentious issues.

5.2.6 Incident Management and Breach Reporting

Staff must be aware of their department's arrangements that are in place to identify, report (via Datix), manage and resolve any data breaches within specified legal timescales (presently 72 hours). Lessons learnt will be shared to continually improve procedures and services, and consideration given to updating risk registers accordingly. Incidents must be reported immediately following local reporting arrangements.

5.2.7 Information Governance Compliance

All information asset owners and departments must have monitoring arrangements in place to ensure that personal and sensitive data is being used appropriately and lawfully.

5.2.8 Intellectual Property

Intellectual property created by an NHS Wales Organisation remains the property of that organisation. Unpublished documents created by the NHS Wales Workforce must not be published or made available to any individual not employed by the NHS in Wales 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 NHS Wales organisations by the NHS Wales Workforce during the course of their employment will remain the property of the organisation.

5.3 Records Management

Cardiff and Vale University Health Board (the UHB) understands the definition of records to be:

"Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business". *Reference BS ISO 15489.1*

"An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees including consultants, agency or casual staff." *Reference. Department of Health Records Management: NHS Code of Practice Part 1*

All records held by the UHB fall within the scope of this policy as these are either personal (relating to patients, public and employees) or corporate (for example financial records, letters, reports) and regardless of whether they are held in electronic, virtual or physical format. It applies to all areas and services within the remit of the UHB.

The UHB is committed to the handling and processing of all health records in accordance with the legal requirements, codes of practice and guidance issued by relevant authorities including, but not restricted to, the Welsh Government and the Information Commissioner's Office.

To achieve this, the UHB and its employees will follow the Records Management Code of Practice for Health and Social Care 2022

All staff should understand and be aware of the importance attached to the way in which records are managed and the relationship of records management to assist in achieving the overall business strategy of the organisation.

Records will be managed in accordance with the UHB's Records Management Retention and Destruction Protocol and Schedule.

5.4 Access to Information

The UHB is in some circumstances required by law to disclose information. Examples include information requested under:

- Freedom of Information Act 2000
- Environmental Information Regulation 2004
- General Data Protection Regulation

For further detail, please see the below links or contact the Information Governance department.

Freedom of Information Act 2000 and Environmental Information Regulations 2004 Procedure

Dealing with Subject Access Requests under Data Protection Legislation Procedure

All staff have a responsibility to provide information for where requested to do so by the Information Governance team.

Processes must be in place for disclosure under these circumstances. Where required, advice should be sought from the UHB's information governance department.

5.5 Confidentiality

5.5.1 Confidentiality: Code of Practice for Health and Social Care in Wales

The UHB has adopted the Confidentiality: Code of Practice for Health and Social Care in Wales. All staff have an obligation of confidentiality regardless of their role and are required to respect the personal data and privacy of others.

Staff must not access information about any individuals who they are not providing care, treatment or administration services to in a professional capacity. Rights to access information are provided for staff to undertake their professional role and are for work related purposes only. It is only acceptable for staff to access their own record where self-service access has been granted.

Appropriate information will be shared securely with other NHS and partner organisations in the interests of patient, donor care and service management. (See section 5.6 on Information Sharing for further details).

It may be pertinent to discuss cases with colleagues for professional reasons (to gain advice, or share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the individual concerned.

5.6 Sharing Personal Data

5.6.1 Wales Accord for the Sharing of Personal Information (WASPI)

The WASPI Framework provides good practice to assist organisations to share personal data effectively and lawfully. WASPI is utilised by organisations directly concerned with the health, education, safety, crime prevention and social wellbeing of people in Wales. << http://www.waspi.org/nhs >>

The UHB will use the WASPI Framework for any situation that requires the regular sharing of information outside of NHS Wales wherever appropriate. Advice must be sought from the information governance department in such circumstances.

5.6.2 One-off Disclosures of Personal Data

Formal Information Sharing Protocols (ISPs) or other agreements must be used when sharing information between external organisations, partner organisations, and external providers acting in the capacity of a data controller. ISPs provide a framework for the secure and confidential obtaining, holding, recording, storing and sharing of information. Advice must be sought from the information governance department in such circumstances.

Personal data may need to be shared externally on a one-off basis, where an ISP or equivalent sharing document does not exist. Advice must be sought from the information governance department in such circumstances.

5.6.3 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. Members of the Workforce should exercise their professional judgement in such circumstances. NHS Wales Organisations should support the Workforce to make appropriate decisions by providing support, guidance and training.

5.7 Welsh Control Standard for Electronic Health and Care Records

5.7.1 The Control Standard

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, and provides the mechanism through which organisations commit to them. NHS Wales organisations have committed to abide by the Control Standard. The Control Standard will be underpinned by local level policies and procedures to ensure electronic records are accessed and used appropriately.

5.8 Data Quality

Key components of data quality include; accuracy, completeness, validity, timeliness, free from duplication or fragmentation, defined and consistent. Data from all areas should be recorded and processed at all levels in the Health Board using relevant skills and knowledge.
The Health Board has set 8 key objectives in order to achieve the policy aims. They are:

1. Data is accurate and up to date:
   - Correct and accurately reflects what actually happened
   - Precise and includes all data processed in the organisation

2. Data is complete: Data should be captured in full and where applicable a valid and traced NHS number must be included to support operational use.

3. Data is valid
   - Data should be held in a format which conforms to recognised national standards
   - Must be mapped by codes to national values where these are in existence
   - Held in computer systems that are programmed to only accept valid entries wherever possible

4. Data is timely
   - Data should be collected at the earliest opportunity, preferably at the time and place of the activity taking place
   - Data is available when required for its intended use

5. Data is free from duplication and fragmentation: Patients must not have duplicated or confused patient records e.g. should not have two or more separate records held on Patient Management Systems.

6. Data is defined and consistent: The data being collected should be understood by the staff collecting and interpreting it.

7. Coverage: Data from all areas of activity - clinical or corporate should be recorded in the appropriate place and format.

8. Data quality management: At every level across the Health Board those managing data quality must have the appropriate skills and knowledge.

5.9 Data and Technical Standards

The UHB will adopt and comply with the standards set out in Welsh Health Circulars, Data Set Change Notices and the Welsh Data Dictionary.

The UHB will adopt the WTSB technical standards as they are produced for all new systems and upgrades, and information asset owners should be establishing development programmes for systems to be fully compliant by 2023.

Asset owners will ensure that the data and images are made available to the UHB's clinical data repository, via a method agreed with the corporate informatics department.

6. Information Security

6.1 Purpose of Security Procedures

The purpose of an IT Security protocol is to preserve:

- Confidentiality — access is confined to those with authority to view the data.
- Integrity — all systems are working in the way they were intended to work.
- Availability — information is delivered to the right person, when it is needed.

6.2 User Access Controls

Access to information will be controlled on the basis of business requirements.

System Managers will ensure that appropriate security controls and data validation processes, including audit trails, will be designed into application systems that store any information, especially personal data. The system manager for any given system will be the corresponding Information Asset Owner.

The workforce has a responsibility to access only the information which they need to know in order to carry out their duties. Examples of inappropriate access include but are not restricted to:

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

User access will be regularly monitored using NIIAS for all national systems. Inappropriate access can result in disciplinary action in line with the Health Board's policy and procedures. In some cases, inappropriate access can even result in criminal prosecution by the Information Commissioner or by the Director of Public Prosecutions.

Employees who are asked to access information relating to colleagues, friends or relatives need to declare their relationship to their line manager, who will decide if the task could be carried out by another staff member.

6.2.1 Physical Access Controls

Maintaining confidentiality in clinical areas can be challenging and the need to preserve confidentiality must be carefully balanced with the appropriate care, treatment and safety of the patient.

Individuals, departments and Information Asset Owners are responsible for determining the relevant security measures required based on local risk assessment.

All reasonable steps should be taken to ensure high standards of security in areas where data is kept. As a minimum, offices, vehicles and computers should be locked when the user is absent. Access cards, PIN codes, key codes, etc. must be kept secure and regularly changed as required.

All central file servers and central network equipment will be located in secure areas with access restricted to designated staff as required by their job function.

6.2.2 Passwords

The workforce are responsible for the security of their own passwords which must be developed in line with NHS guidance ensuring they are regularly changed. Passwords must not be disclosed to anyone. Recognising that, at the current time, the UHB still has a limited number of generic accounts, users will be held fully responsible and accountable for any infringement and breaches of data protection legislation where they have shared their log in details.

In the absence of evidence to the contrary, any inappropriate access to a system will be deemed as the action of the user. If a user believes that any of their passwords have been compromised, they must change them immediately.

Staff must not logon to any computer system using another member of staff's log in details and password.

6.2.3 Remote Working

NHS Wales recognises that there is a need for a flexible approach to where, when and how our workforce undertake their duties or roles. Handling confidential information outside of your normal working environment brings risks that must be managed.

Examples of remote working include, but are not restricted to:

- Working from home
- Working whilst travelling on public/shared transport
- Working from public venues (e.g. coffee shops, hotels etc.)
- Working at other organisations (e.g. NHS, local authority or academic establishments etc.)
- Working abroad

As a control measure to mitigate risks involved in remote working, no member of the workforce will work remotely unless they have been authorised to do so. Remote working must not be authorised for anyone who is not up to date with mandatory training in information governance.

6.2.4 Staff Leavers and Movers

Managers will be responsible for ensuring that local leaving procedures are followed when any member of the workforce leaves or changes roles to ensure that user accounts are revoked / amended as required and any equipment and/or files are returned. Confidential, patient or staff information must not be transferred to a new role unless authorised by the relevant heads of service. A leaver's checklist should be completed in all cases.

6.2.5 Third Party Access to Systems

Any third party access to systems must have prior authorisation from both the IT and IG departments.

6.3 Storage of Information

All information stored on or within the UHB is the property of the UHB, unless there are contractual agreements that state otherwise. For legal purposes the UHB should be informed of, and agree to, all arrangements where we are hosting an information asset but are not the asset owner. An example of this is information stored in an email, which has been sent by a member of staff, but not in their capacity as an employee of Cardiff and Vale UHB (e.g. on trade union, University or Royal College business)

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

Wherever possible, personal information should be stored on a UHB secure server. If it is to be stored outside a secure server (e.g. laptop c drive, flash stick): - the computer / device should be password protected and the data encrypted. The storage of personal data in the "Cloud" presently requires approval by the Welsh Information Governance Board

All systems should be backed up as part of an agreed backup regime. Where business critical information is held on local hard drives, portable devices or removable media, the IT department must be informed and agreements on how to back up the data reached.

Staff must:

- Ensure that all data is saved to network servers and not to the local device hard drive.
- Ensure that when leaving computers unattended for any length of time they either switch them off, lock the screen or log themselves off. Computers must not be left unattended or accessible to others.
- Staff must ensure that they use the information they have access to in an appropriate manner at all times.

6.4 Portable Devices and Removable Media

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

Portable devices include, but are not limited to, laptops, tablets, Dictaphones®, mobile phones and cameras. Where a portable device offers the functionality of a lock-screen, it is the responsibility of the user to ensure this functionality is securely activated.

All portable devices must either be encrypted, or access the network via NHS Wales approved applications (e.g. Mobile Device Management Software).

Users must ensure that all portable devices are physically connected (plugged in) to the UHB's network every 4 weeks and that all upgrades and cyber patches are updated at this time. Upgrades via wifi are not acceptable at the present time due to affordability and available bandwidth.

Users must not attach any personal (i.e. privately owned) portable devices to any NHS organisational network without prior authorisation.

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

All removable media such as CDs must be encrypted if used to transport confidential information and should only be used if no other secure method of transfer is available. Users must not send details of how to unencrypt with the removable media.

6.5 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.

6.5.1 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.

6.5.2 Electronic

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

6.5.3 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 your information governance team.

6.6 Transporting and relocation of information

6.6.1 Transporting Information

When information is to be transported from one location to another location, local procedures must be formulated and followed to ensure the security of that information.

6.6.2 Relocating information

When information is to be relocated to another location, local procedures must be formulated and followed to ensure no information is left at the original location.

6.7 Security of Assets

The UHB will maintain an inventory of the major assets associated with its information systems. Assets will include:

- Physical assets
- Software applications
- Data
- Back-ups

6.7.1 Physical Assets

Protection of IT equipment (including that used off site) is necessary both to reduce the risk of unauthorised access to data and to safeguard against loss or damage.

Data Centre's both local and national servers must be protected from power failures through use of uninterruptible power supplies (UPS), with backup generator power.

Ongoing maintenance arrangements are the subject of contractual agreement and only approved system engineers are allowed access to hardware.

Details of all faults on "maintained" equipment will be recorded by the UHB's IM&T Help Desks.

6.7.2 Software Applications

The IM&T Department will monitor all systems and PCs to ensure that all proprietary software products on the Local Area Network are used legally, licenced, and use SNOW as a Software Asset Management (SAM) solution.

In general the number of software installations of a given application e.g. Microsoft Office version xx cannot exceed the number of licences for that application held by the organisation. The UHB has purchased software specifically to monitor levels of usage of all software applications on the network. Regular reviews will be undertaken to ensure adequate licensing.
Copying of proprietary or organisational software, for use on computers that do not belong to the UHB, for any purpose other than authorised business, may infringe copyright and may be in breach of organisational policy. Copying of software in these circumstances may lead to disciplinary action.

Only software licensed to the UHB may be used on UHB equipment. Although it is not strictly illegal to use software legitimately belonging to an individual the installation and use of such software will not be permitted on any UHB equipment.

In the event of a dispute on the authorised validity of software the IM&T Security Manager has the authority to order the removal of any software from UHB equipment.

Software procured from academia cannot be loaded onto an NHS device i.e. students are not able to load university software onto the UHB device due to licencing restrictions.

Free software is not to be downloaded onto UHB computers due to the risk of malware, viruses and trojan's being introduced and affecting the network.

Staff need to remember that the same restrictions and requirements apply when utilising UHB IT equipment and working at home.

6.7.3 Data

Equipment (e.g. PCs, Laptops), data and software can be taken off-site but requires authorisation by the appropriate line manager.

Data must be saved to network servers and not to the local devices hard drive.
All laptops must be encrypted.

The destruction of data can only be authorised by the manager of the relevant system that the data is stored on, and "routed" via procurement.

Any storage media (e.g. hard disk, CD-ROM, diskette, magnetic or DAT tape) can only be disposed of after reliable precautions to destroy the data have been taken, and routed via procurement.

6.7.4 Back-ups

It is the responsibility of individual users to back up any systems that do not store their data centrally. The IM&T Department undertakes to back up on a daily basis the Network Servers and all centrally held data and will maintain detailed data housekeeping procedures for all systems they are responsible for. Back-up and archive data will be accorded the same security as live data. All back-ups and archived data will be held off-site at CRI. Back-up data should be able to provide an adequate level of service and recovery time in the event of an emergency.

The IM&T Security Manager and all relevant managers and staff must be informed prior to any recovery from back-up data.

6.8 Security Incidents

An IM&T security incident is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact, for example
- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of UHB business
- An embarrassment to the UHB

All incidents or information indicating a suspected or actual security breach should initially be reported to the immediate Line Manager and logged on the incident reporting system (e-Datix). In addition, the IT Security Manager or Information Governance Department should be informed for them to determine

whether an actual security breach has taken place. Further comprehensive guidance will be developed to support this.

6.9 Business Continuity Planning and Risk Assessment

Business continuity planning is an organisational issue.

All Clinical Board areas will ensure that they have developed, maintained and tested adequate business continuity plans which will cover the following:

- A documented assessment of how long their users could manage without the relevant UHB system they depend on
- A documented assessment of the criticality of the loss of their system, including the impact of the short, medium and long term on UHB business activities
- Identification and agreement of all responsibilities and emergency arrangements
- Documentation of agreed procedures and processes
- An assessment of how resilience and continuity will be achieved.

The IM&T Department will ensure that it has an up-to-date Business Contingency/Disaster Recovery Plan in place that assesses the criticality of the loss of all systems managed and maintained by the IM&T Department.

6.10 The Network & Information Systems (NIS) Regulations

The Network & Information Systems Regulations 2018 (NIS Regulations) provides a legal framework to bolster the level of cyber and physical security of networks and information systems for the provisions of essential services and digital services.

The NHS is considered an Operator of Essential Services (OES) and as a Competent Authority, Welsh Ministers are responsible for overseeing the operation of the NIS Regulations. The NHS Wales Cyber Resilience Unit (CRU), hosted with DHCW provide guidance and support to Welsh Ministers.

To comply with NIS Regulations, all new implementations of a ‘critical system’ must be assessed by the Cyber Security Department against the Cyber Assessment Framework.

6.11 Suppliers of third-party systems

All suppliers who host or access UHB data need to comply with the Welsh Health Circular guidance on Cyber security and information governance (WHC/2017/025). For guidance on this Welsh Health Circular, please contact CV.IMT.Security@wales.nhs.uk

7. Use of the internet

7.1 Position Statement

Internet access is provided to staff to assist them in the performance of their duties. The provision of these facilities represents a major commitment on the part of the UHB in terms of investment and resources.

All members of staff should become competent in using internet services to the level required for their role in order to be more efficient and effective in their day-to-day activities.

The UHB will support its workforce in understanding how to safely use internet services and it is important that users understand the legal, professional and ethical obligations that apply to its use. If used correctly, the internet can increase efficiency and safety within patient care.

7.2 Conditions & Restrictions on Internet Use

To avoid inadvertent breaches of this policy, inappropriate content will be blocked by default where possible. Inappropriate material must not be accessed. Exceptions may be authorised for certain staff where access to particular web pages are a requirement of the role. Subject matter considered inappropriate is detailed in the appendix.

Some sites may be blocked by default due to their general impact on network resources and access to these for work purposes can be requested by contacting the Local IT Service Desk.

Regardless of where accessed, users must not participate in any online activity or create or transmit or store material that is likely to bring the organisation into disrepute or incur liability on the part of NHS Wales.

Business Sensitive Information or Personal Data (which includes photographs and video recordings) of any patient, member of the public, or member of staff taken must not be uploaded to any form of non-NHS-approved online storage, media sharing sites, social media, blogs, chat rooms or similar, without both the authorisation of a head of service and the consent of the individual who is the Data Subject of that recording. The NHS Wales Social Media Policy provides information on the appropriate use of social media.

It is each user's responsibility to ensure that their internet facilities are used appropriately.

7.3 Personal Use of the Internet

The UHB allows staff reasonable personal use of internet services providing this is within the bounds of the law and decency and compliance with policy.

Personal use should be incidental and reasonable and should be included in your personal time. In addition to this, users must not stream or download large volumes of data (e.g. streaming audio or video, multimedia content, software packages) as these may have a negative impact on network resources.

Staff must not load software packages onto their PC's or laptop's without authorisation from the IM&T Security Office. On no account must 'games software' be loaded on staff PC's or laptops.

Staff members are encouraged to use the CAV free Wi-Fi facilities by default on personally-owned devices.

Staff who use NHS equipment outside NHS Wales premises (for example – in a home environment) are permitted to connect to the internet. Use of the internet under these circumstances must be through a secure VPN connection provided by the UHB. Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy.

All personal use of the internet is carried out at the user's own risk. The UHB does not accept responsibility or liability for any loss caused by or liability arising from personal use of the internet.

Internet access facilities must not be used to run or support any kind of paid or unpaid personal business venture outside work, whether or not it is conducted in a user's own time or otherwise.

8. Email

8.1 Use of NHS Wales email account

All UHB staff, must use their assigned NHS Wales email account when conducting UHB business. The use of private accounts, such as @gmail, @AOL and @doctors.org are not permitted when communicating any UHB activity such as, but not limited to: patient, staff or business sensitive data.

8.2 Inappropriate emails

Inappropriate content and material must not be sent by email. Inappropriate content including prohibited language in emails may be blocked. Subject matter considered inappropriate is detailed in the appendix.

Regardless of where accessed, users must not use the UHB's email system to participate in any activity, to create, transmit or store material that is likely to bring the UHB into disrepute or incur liability on the part of the UHB.

Some users may need to receive and send potentially offensive material as part of their role (for example - child protection). Arrangements must be authorised to facilitate this requirement.

8.3 Personal Data and Business Sensitive Information: Filtering and Misdirection

The NHS Wales network is considered to be secure for the transfer of any information including personal data and business sensitive information within NHS Wales and organisations with Transport Layer Security (TLS) enabled. This includes all email addresses within the NHS email directory that end in "wales.nhs.uk", which are hosted on the NHS Wales email service and the email services of TLS enabled organisations as listed on HOWIS. The list can be accessed here:

TLS Assurance (sharepoint.com)

Whilst it is safe and secure to transfer personal data between these addresses without encryption or passwords, the user must have a lawful basis for doing so. Please note that universities are not included in this list.

Transfer of personal data or business sensitive information between any email address not ending in "wales.nhs.uk", or TLS enabled is not currently considered secure. Where this type of information needs to be sent, appropriate security measures must be implemented. For example, the information should be sent via the Secure File Sharing Portal or via email with an appropriate level of encryption.

Users must be vigilant in ensuring that all emails are sent to the correct recipient and must check that the correct email address is used, for example by checking the NHS Wales email address book. Even where the recipient email address is considered secure, as a mitigating factor to avoid any inadvertent misdirection, encryption of any email attachment containing sensitive data should be considered. Misdirected emails should be reported via local incident reporting processes.

8.4 Personal Use of Email

The UHB allows staff reasonable personal use of their email account providing this is within the bounds of the law and decency and compliance with policy.

Personal use should be incidental and reasonable and should be included in your personal time. It is a requirement that you mark personal emails as personal in the subject heading. In doing so, staff should recognise that these emails will be monitored and may be subject to Information Access requests made to the UHB. Staff members are therefore strongly encouraged to use their personal email accessed via CAV free Wi-Fi facilities by default on personally-owned devices.

Staff who use NHS equipment outside NHS Wales premises (for example – in a home environment) are permitted to send personal emails. Use of the email under these circumstances must be through a secure VPN connection provided by the UHB. Use of the equipment for such purposes is still subject to the same conditions as laid out in this policy.

All personal use of email is carried out at the user's own risk. The UHB does not accept responsibility or liability for any loss caused by or liability arising from personal use of email.

The UHB's email must not be used to run or support any kind of paid or unpaid personal business venture outside work, whether or not it is conducted in a user's own time or otherwise.

On occasion, suppliers may offer discounts that require UHB staff to validate their NHS employment, by subscribing via an NHS email accounts. The UHB does not wish to disadvantage staff by prohibiting this validation step. However, it is expected that any offers that are subscribed to must be decent, lawful and appropriate to a professional environment, Additionally, the subscription should not hinder the performance of the individuals job role.

8.5 Records Management and Access to Information requests in respect of Email

Staff are encouraged not to use the email system as a storage facility. By design, all emails should either be deleted or saved securely to the appropriate record (e.g. to a clinical / business record or network drive).

Information held on computers, including those held in email accounts may be subject to requests for information under relevant legislation and regulation. As such any staff member who stores data in email folders should comply with section 5.2.1.1 Information Asset Registers.

All staff should be mindful that it may be necessary to conduct a search for information and this may take place with or without the author's knowledge or consent.

9. Training and Awareness

Information governance is everyone's responsibility. Training is mandatory for UHB staff and must be completed at commencement of employment and at least every two years subsequently. Non-NHS employees must have appropriate information governance training in line with the requirements of their role.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact their local Information Governance Department.

The UHB's 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.

In order to ensure that this work is successfully supported and completed, there must be robust IGT programmes in place. To this effect, managers will:

- Complete training needs analyses for all staff as part of mandatory training in line with the Information Governance Training Programme Framework
- Manage staff training attendance -for new staff and refresher training
- Maintain ESR and local training records
- Identify and implement refresher training where incidents and poor performance has been identified

The arrangements for regular monitoring compliance are as follows:

- Overall compliance – to the DHIC via the SIRO
- Local compliance – to the clinical board performance reviews by clinical board directors
- Corporate arrangements – to the DHIC via the SIRO
- Compliance by formal assessment:
    - Health and Care Standards 3.4 and 3.5
    - Caldicott annual assessment - Internal Audits sponsored by the DHIC
    - Annual and specific audits by the Welsh Audit Office
    - Any other audits or assessments directed by the Welsh Government

10. Monitoring and compliance

The UHB trusts and respects the privacy of its employees and does not want to interfere in their personal lives. However, it reserves the right to monitor work processes to ensure the effectiveness of the service as a legitimate business interest. This will mean that any personal activities that the employee practices in work may come under scrutiny.

The UHB uses software to automatically and continually record the amount of time spent by staff accessing the internet and the type of websites visited by staff. Attempts to access any prohibited websites which are blocked is also recorded.

The UHB uses software to scan emails for inappropriate content and filters are in place to detect this. Where an email is blocked, emails may be checked for compliance when a user requests an email to be released. All email use will be logged to display date, time, username, email content; and the address to which the message is being sent.

Staff should be reassured that the UHB will take a considered approach to monitoring. However, it reserves the right to adopt different monitoring patterns as required. Monitoring is normally conducted where it is suspected that there is a breach of either policy or legislation. Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the employee.

Managers are expected to speak to staff of their concerns should any minor issues arise. If breaches are detected, an investigation may take place. Where this or another policy is found to have been breached, disciplinary procedures will be followed.

Concerns about possible fraud and or corruption should be reported to the counter fraud department.

In order for the UHB to achieve good information governance practice staff must be encouraged to recognise the importance of good governance and report any breaches to enable lessons to be learned. They must be provided with the necessary tools, support, knowledge and training to help them deliver their services in compliance with legislation. Ultimately, a skilled workforce will have the confidence to challenge bad information governance practice and understand how to use information legally in the right place at the right time. This should minimise the risk of incidents occurring or recurring.

11. Review

This policy will be reviewed every two years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Practice change or change in system/technology; or
- Changing methodology.

12. 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.

13. Documents to read alongside this Procedure

- Records Management Procedure
- Records Management Retention and Destruction Protocol and Schedule
- Information Governance Policy and Framework
- Data Protection Act Policy and Procedures
- Freedom of Information Act Procedure
- Risk Management Policy
- Information Risk Management Procedure
- Guide to Incident Reporting Incident Management Investigation and Reporting. [Serious incidents]
- Electronic and Paper Clinical Results Review and Retention Protocol
- Records Management Code of Practice for Health and Social Care 2016
- Data Quality Operational Management and Responsibilities
- Records Management Policy
- Records Management Retention and Destruction Protocol
- Validation at Source System (VASS) checks mandated by Welsh Government.
- Data Standard Change Notifications (DSCNs) issued by the National Wales Informatics Service
- Other relevant documents mandated by Welsh Government

Appendix: Inappropriate use

For the avoidance of doubt, the UHB 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 without the relevant permission. 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 email 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 or saving any information or images which are unlawful, or could be regarded as defamatory, offensive, abusive, obscene, hateful, pornographic, violent, terrorist, indecent, being discriminatory in relation to the protected characteristics, or using the email system to inflict bullying or harassment on any person.
- 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 the UHB 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 an 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;
    - 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.

Annex 1: Policy Development - Version Control

Revision History

Date	Version	Author	Revision Summary
1/8/18	-	Andrew Fletcher, NWIS	NWIS policy documents for Information Governance, Information Security, Internet Use and Email Use
15/8/18	V0.1	Andrew Nelson	Amendments to draw documents together and include UHB 12 commandments, local variation and requirements for adoption of technical and data standards
17/8/18	V0.2	PJR, JW & AVN	Inclusion of DQ, data standards and medical records. Clarification of information ownership in respect of data stored on UHB network
15/11/2019	V0.3	JW & DJ	Incorporation of all-Wales Email Policy.
08/01/2024	V0.4	JW & DJ	The inclusion of additional UK GDPR definitions Guidance on the use of online forms used to collect personal data A new statement explaining that unlawful access to personal data can result in disciplinary action and criminal prosecution A new clause on the Network & Information Systems Regulations and Welsh Health Circular guidance An explicit requirement to use NHS email to conduct UHB business Clarification on the use of NHS email to receive discounts

Reviewers

This document requires the following reviews:

Date	Version	Name	Position

Approvers

This document requires the following approvals:

Date	Version	Name	Position

Annex 2: Equality Impact Assessment

Equality Impact Assessment (EQIA) Form		
Ref no: POL/IGMAG/IG/v1		
Name of the policy, service, scheme or project:	Service Area	
C&V Information Governance Policy	Information Governance	
Preparation		
Aims and Brief Description	The policy is a new All Wales Information Governance Policy. The policy will replace all local policies in this area.	
Which Director is responsible for this policy/service/scheme etc	Adaptation of existing policies and the NWIS policy	
Who is involved in undertaking the EQIA		
Have you consulted with stakeholders in the development of this policy?	*Yes. A sub group has developed this policy with a membership consisting of information governance leads and an OSSMB representative. IM&T leads and the Wales Partnership Forum have been consulted.* *The NHS Wales Information Governance Management and Advisory Group have approved the text of this Policy. The policy will be approved by the Wales Information Governance Board.*	
Does the policy assist services or staff in meeting their most basic needs such as; Improved Health, fair recruitment etc	*Yes. The policy will provide consistency throughout NHS Wales in having a single policy. This will ensure that staff who work across boundaries have a consistent standard to work to, hence strengthening the governance framework. A key driver during the process was the need to recognise that organisations needed to trust their staff.*	
Who and how many (if known) may be affected by the policy?	*All NHS Wales staff within the Health Boards and NHS Trusts.*	
What guidance have you used in the development of this service, policy etc?	*The policy is based on good practice and legal obligations as set out by the Information Commissioners Office and in the legislation. The policy has also been constructed from existing agreed principles and the corporate knowledge of its stakeholders.*	

Equality Duties

The Policy/service/project or scheme aims to meet the specific duties set out in equality legislation.	Protected Characteristics										
	Race	Sex/Gender	Disability	Sexual orientation	Religion and Belief	Age	Gender reassignment	Pregnancy and Maternity	Marriage & civil	Welsh Language	Carers
To eliminate discrimination and harassment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote equality of opportunity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Promote good relations and positive attitudes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Encourage participation in public life	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
In relation to disability only, should the policy / service / project or scheme take account of difference, even if involves treating some individuals more favourably?							✓				

Key	
✓	Yes
x	No
-	Neutral

Human Rights Based Approach – Issues of Dignity & Respect

The Human Rights Act contains 15 rights, all of which NHS organisations have a duty. The 7 rights that are relevant to healthcare are listed below.

Consider is the policy/service/project or scheme relevant to:	Yes	No	N/A
Article 2: The Right to Life	X		
Article 3: the right not to be tortured or treated in a inhumane or degrading way	X		
Article 5: The right to liberty	X		
Article 6: the right to a fair trial	X		
Article 8: the right to respect for private and family life	X		
Article 9: Freedom of thought, conscience and religion	X		
Article 14: prohibition of discrimination	X		

Measuring the Impact

What operational impact does this **policy, service, scheme or project**, have with regard to the Protected Characteristics. Please cross reference with equality duties

	Impact – operational & financial
Race	This is a high level framework approach which aims to achieve the values under the policy, it is the protection of everybody's information and gives clear guidelines. The policy details how the organization protects someone's data and security without prohibiting access to services and providing adequate access to data to meet individual needs and the appropriate sharing of data.
Sex/gender	
Disability	
Sexual orientation	
Religion belief and non belief	
Age	
Gender reassignment	
Pregnancy and maternity	
Marriage and civil partnership	

Other areas	
Welsh language	
Carers	

Outcome report

Equality Impact Assessment: Recommendations Please list below any recommendations for action that you plan to take as a result of this impact assessment						
Recommendation		**Action Required**	**Lead Officer**	**Time-scale**	**Resource implications**	**Comments**
1	Communication of the changes	Make sure staff aware of the changes	AF	ASAP	Time	

Recommendation	Likelihood	Impact	Risk Grading
1	2	2	4
2	2	2	4

Risk Assessment based on above recommendations

Reputation and compromise position	**Outcome**
It is providing security and reassurance to stakeholders that the information we hold is used appropriately and any breach may lead to fines and reputational damage.	To ensure that information is used and protected appropriately and a framework in place to ensure that happens.
Training and dissemination of policy	
More training and dissemination in Health Boards on this policy.	

Is the policy etc lawful?	**Yes** ☒	**No** ☐	**Review date**
Does the EQIA group support the policy be adopted?	**Yes** ☒	**No** ☐	**3 years**
Signed on behalf of C&V Equal Impact Assessment Group	S Brooks	Lead Officer	
Date:	8 May 2018	Date: 8 May 2018	

	1	2	3	4	5
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**

Statutory duty	No or minimal impact or breach of guidance / statutory duty Potential for public concern Informal complaint Risk of claim remote	Breech of statutory legislation Formal complaint Local media coverage – short term reduction in public confidence Failure to meet internal standards Claims less than £10,000 Elements of public expectations not being met	Single breech in statutory duty Challenging external recommendations Local media interest Claims between £10,000 and £100,000 Formal complaint expected Impacts on small number of the population	Multiple breeches in statutory duty Legal action certain between £100,000 and £1million Multiple complaints expected National media interest	Multiple breeches in statutory duty Legal action certain amounting to over £1million National media interest Zero compliance with legislation Impacts on large percentage of the population Gross failure to meet national standards

Risk Grading Descriptors

LIKELIHOOD DESCRIPTION	
5 Almost Certain	Likely to occur, on many occasions
4 Likely	Will probably occur, but is not a persistent issue
3 Possible	May occur occasionally
2 Unlikely	Not expected it to happen, but may do
1 Rare	Can't believe that this will ever happen