Health Education and Improvement Wales (HEIW)

Records Management Policy

Policy Owner: Head of Cyber Security & Information Assurance
Approved by: Executive Team
Issue Date: 29 January 2025
Review Date: 29 January 2028
Date of EIA Outcome: 9 September 2024

Contents

1. Policy Statement 3
2. Scope 3
3. Aims and Objectives 4
4. Roles and Responsibilities 4
5. Policy 6
    5.1. General Conditions 6
    5.2. Collection 7
    5.3. Definition of a Record and Document 8
    5.4. Usage 8
    5.5. Storage 9
    5.6. Access 9
    5.7. Transfer 9
    5.8. Retention 10
5.9. Disposal 12
6. Definitions 13
    6.1. Record 13
    6.2. Document 13
    6.3. Personal Data 13
    6.4. Special Category Data 13
    6.5. Processing 14
    6.6. Lawful Basis for Processing Personal Data 14
    6.7. Individual Rights 15
    6.8. Data Protection Impact Assessment (DPIA) 15
    6.9. Information Asset 15
    6.10. Information Asset Register 15
7. Equality Impact Assessment 16
8. Awareness and Training 16
9. References 16
10. Getting Help 17
11. Legislation and Standards 17
12. Related Policies and Procedures 18
13. Publication and Dissemination of Organisation Wide Documents 18
14. Compliance 18
15. Policy Review 19
Appendix A 20

1. Policy Statement

HEIW's Records Management Policy sets out key areas of responsibility and affirms our commitment to achieving high standards in records management. As a Special Health Authority (SHA), the correct management of records is a legal and compliance matter under Data Protection Legislation (UK GDPR and DPA 2018); the Freedom of Information Act 2000 (FOIA); and the Public Records Act (PRA).

Information is a valuable commodity and essential to HEIW's day-to-day operations, carrying out its role and statutory functions. HEIW receives, creates, manages, and processes a significant volume of information and in a range of formats (e.g., electronic, physical).

Appropriate and effective records management is therefore considered a critical business activity, to ensure that records and the information they contain are appropriately managed, accurate, up-to-date, and available to authorised individuals when required, and in a way which conforms with HEIW's legal obligations.

HEIW recognises that specific procedures within departments may diverge, and for that reason this policy should be examined in conjunction with any such policies and procedures and not read in isolation.

2. Scope

This policy applies to all physical and electronic information assets created, owned, and managed by HEIW. It covers the collection, use, retention, storage, transferring, and destruction of information.

It applies to HEIW's workforce including staff, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of HEIW. It encompasses all forms of information processed by HEIW; and covers all business functions and the information, information systems, networks, physical environment, and relevant people who support those business functions.

3. Aims and Objectives

This policy aims to set out key areas of responsibility for records management and achieving exacting standards in records management in accordance with HEIW's legal obligations.

HEIW recognises its corporate responsibility and commitment to compliance with records management requirements as stated within statutory provisions, relevant codes of practice and good practice guidance.

This policy for that reason aims to deliver the following key outcomes to ensure effective records management:

- records and the information they contain shall be managed appropriately throughout the 'record lifecycle'.
- records shall be managed in a way which complies with HEIW's legal obligations.
- records and the information they contain will be recorded on an Information Asset Register (IAR).
- records and the information they contain must only be held for as long as they're required.
- appropriate retention schedules outlining the period of retention for records HEIW holds must be defined.
- records are appropriately managed, accurate, up-to-date, and available to authorised individuals when required.
- records and the information they contain are appropriately protected.
- all staff are aware of their roles and responsibilities in relation to records management.

4. Roles and Responsibilities

The **Chief Executive (CEO)** 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. Specific responsibilities will be delegated to the Data Protection Officer, Senior Information Risk Officer and the Caldicott Guardian or an Executive Director as appropriate.

The **Senior Information Risk Owner (SIRO)** is responsible for information risk management across the organisation. The SIRO is responsible for taking ownership of the organisation's information risk policy and advocating crucial information risk management and practice. The SIRO reports to the CEO and is accountable to the Board. HEIW's nominated SIRO is the Board Secretary.

The **Caldicott Guardian** is responsible for protecting the confidentiality of health and care information held by their respective organisation and enabling appropriate information sharing by ensuring that information is used properly. Together with the respective Senior Information Risk Officer, they are responsible for monitoring the process by which all information assets are identified, managed and reviewed. Although HEIW does not deal with patient information it has been agreed this role shall be held by the Medical Director.

The **Data Protection Officer (DPO)** reports to the CEO and is accountable to the Board. The DPO will provide oversight of HEIW compliance with data protection legislation and informing the organisation on its data protection obligations. A data protection expert, the DPO must maintain expert knowledge of data protection laws and practices and how these apply to an organisation. The DPO will be the primary point of contact within the organisation regarding data protection matters, whilst advising senior management on the development and establishment of policies, standards, procedures, and other measures to ensure effective governance and compliance with data protection legislation. HEIW's nominated DPO is the Director of Digital, Data and Engagement.

Executive Directors are responsible for the management of information risk within their service areas and are responsible for ensuring their staff and managers are aware of and comply with this policy, any associated HEIW policies, procedures, and work instructions within their directorate.

The **Cyber Security** team are responsible for providing subject matter expertise and guidance on appropriate controls and measures to protect information and information systems.

The **Information Governance** team has a delegated responsibility from the DPO to discharge its duties and carry out necessary operational work to ensure compliance with data protection legislation, NHS Wales policies, standards, procedures, and codes of practice. The Information Governance team are responsible for providing appropriate information governance advice and support to the Information Asset Owners, Service Leads, staff, and managers to ensure the policy is understood and complied with.

Information Asset Owners (IAO's) are responsible for understanding what information is held within their service areas. They are responsible for deciding upon the categorisation of information within their information asset area with support from subject matter experts such as the information governance or cyber security team where required. They can delegate this responsibility to another named individual, but they must retain overall responsibility for the information asset and the correct application of this procedure to that asset. Specific IAO responsibilities are outlined in the Information Asset Procedure.

Managers are responsible for the implementation of this policy and any associated HEIW policies, procedures, and work instructions within their department/directorate. In addition, they must ensure that their staff comply with all relevant policies, understand their responsibilities, and are up to date with mandatory information governance, records management, and cyber security training. Policy breaches must be reported via local incident reporting processes and dealt with in line with the HEIW Disciplinary Policy where appropriate.

All staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. All staff are responsible for their own actions and must:

- comply with this policy and any associated HEIW policies, procedures, and work instructions.
- undertake mandatory ESR information governance, records management, and cyber security training every two years.
- report all data breaches and issues (actual or suspected) to the Information Governance team as soon as possible.
- report any identified information governance risks or concerns within their work area to line management.
- maintain an appropriate level of information governance awareness.

5. Policy

5.1. General Conditions

To ensure appropriate and effective management of records in any form, all staff are responsible for ensuring that records and the information they contain within their own work areas:

- are managed appropriately throughout the 'record lifecycle' from record collection / creation to:
    - use
    - in storage
    - in-transit
    - disposal
    - destruction
- are available to authorised individuals with a legitimate business need for access when required.
- are accurate, maintained and kept up to date throughout the 'record lifecycle'.
- can be accessed by authorised individuals with a legitimate business need for access when required.

- are appropriately secured ‘at-rest’ and ‘in-transit’ using technical, administrative, and/or physical security controls.
- are protected by controls to prevent unauthorised access and processing of information, or accidental loss or damage to the record and the information it contains.
- are created in an electronic form to help minimise the use of paper records.
- are retained for as long as it is necessary and appropriately disposed of when no longer required.
- are made available to those with a legitimate business need considering the ‘need-to-know’ principle.
- are only transmitted to those with a legitimate business need considering the ‘need-to-know’ and ‘need-to-share’ principles.
- can be interpreted correctly and understood by those who have a legitimate business need for access.
- are accurate, can be trusted and integrity and validity can be demonstrated.
- are not misplaced or lost throughout the ‘record lifecycle’.

5.2. Collection

Information is critical to HEIW’s day-to-day operations and carrying out its role and statutory functions. HEIW receives, creates, manages, and processes a significant volume of information and in a range of formats.

When Personal Data is collected, it must be done so with a clear purpose. This must be in line with HEIW’s statutory functions or necessary for the organisation where the lawful basis for doing so has been identified. Any new collection of Personal Data will require the completion of a Data Protection Impact Assessment (DPIA).

When information is collected, an appropriate method of storage must be defined. Information Assets shall for that reason be recorded on an Information Asset Register (IAR).

5.2.1. Information Assets

An Information Asset is considered a body of information (electronic or physical) managed as a single unit so it can be understood, valued, classified, inventoried, protected, managed, and used effectively.

In this context, information assets can refer to any information HEIW considers valuable, important, or critical to its day-to-day operations, decision-making processes, or compliance with regulatory and legal obligations.

Information assets can take many forms including but not limited to:

- Databases
- Files
- Spreadsheets
- Documents
- Organisation Plans
- Registers
- Reports
- Websites

5.2.2. Information Asset Registers

Information Asset Registers (IAR's) are a record of the information assets which are created, owned, and managed by HEIW.

Recording of information assets enables HEIW to remain compliant with local and national information governance requirements, relevant records management codes of practice, and applicable legislation.

5.3. Definition of a Record and Document

A record is information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business.

A document is any piece of written matter in any form, produced or received that provides information or evidence or serves as a record. Some documents will need to be kept as evidence of business transactions, routine activities or as the result of HEIW's legal obligations. These documents must be placed into an official filing system and at this point, they become official records. In other words, records can start off as documents, but not all documents will ultimately become records.

5.4. Usage

Records containing information shall only be used for the purpose the information has been collected. Only authorised individuals with a legitimate business need should have access to records and the information they contain.

For that reason, access to handle and manage information must be centred around the **'need-to-know'** principle. The requirement to share or transfer information must consider the **'need-to-share'** principle. The 'need-to-share' principle is underpinned by a 'need-to-know' (i.e., the potential recipient must have a legitimate business need to use the information).

Personal Data must be processed fairly, lawfully and in a transparent manner. HEIW processes a wide range of Personal Data relating to individuals and in doing so must fulfil its legal obligations set out in Data Protection Legislation. Personal Data refers to any information relating to identified or identifiable living individuals. This includes Personal Data and Special Category Data.

5.5. Storage

All records must be managed appropriately throughout the 'record lifecycle'. Records shall be appropriately stored and protected.

Paper records and the information they contain must be secured under **'lock and key'** using lockable rooms, cupboards, cabinets, or drawers. The use of paper records should however be minimised wherever it is reasonable to do so.

HEIW has adopted a digital-by-default approach and information should therefore be stored electronically wherever possible. Electronic records and the information they contain must be stored in an organised manner using Microsoft SharePoint, Microsoft OneDrive, or an appropriate, authorised system.

Electronic information 'at-rest' must be protected using reasonable and proportionate controls to protect stored information from unauthorised access, modification, or deletion.

All staff are encouraged to contact the Information Governance or Cyber Security teams for any advice and guidance regarding information storage and protection.

5.6. Access

Access to records and the information they contain shall be properly controlled and managed enforcing the 'need-to-know' principle.

Access must therefore be no wider than necessary for the efficient conduct of HEIW work and limited to only authorised individuals with a legitimate business need.

5.7. Transfer

Records and the information they contain must only be shared with authorised individuals with a legitimate business need enforcing the 'need-to-know' and 'need-to-share' principles.

The 'need-to-share' principle is reinforced by the 'need-to-know' principle (i.e., the potential recipient must have a legitimate business need to use the information).

Reasonable and proportionate physical and technical security controls must be put in place to protect information 'in-transit' which is transferred to another organisation or authorised individual.

All staff are encouraged to contact the Information Governance or Cyber Security teams for any advice and guidance regarding information transfer and protection.

5.8. Retention

Records and the information they contain must only be held for as long as they're required. HEIW may need to keep records for a period as specified in relevant records management codes of practice or in accordance with applicable laws and regulations. Records in any format should therefore not be kept beyond their retention period or useful life. An appropriate retention schedule outlining the period of retention for records HEIW holds must for that reason be defined.

Information Asset Owners (IAOs) and their designated deputies have a key responsibility in ensuring that HEIW's information assets are properly recorded, managed, and protected. Therefore, IAOs and their designated deputies are required to:

- record information assets on an Information Asset Register (IAR).
- know the information that is held and the nature of the information.
- understand the risks associated with information assets within their area.
- know the controls and measures in place to preserve the confidentiality, integrity, and availability of their information assets.
- know the details of those who have access and purpose for their access.
- know what the retention period is for the records and the information they contain under their remit.
- know what to do with the records at the end of the defined retention period.

5.8.1. Personal Data

Personal Data must not be kept for longer than is necessary and should be appropriately destroyed of when HEIW no longer have a reason to keep it.

5.8.1.1. Transparency

HEIW holds and processes Personal Data and as such requires Privacy Notices. A privacy notice, also known as a privacy policy, lets individuals know what HEIW is doing with their personal data.

Providing a privacy notice is a key requirement of the UK GDPR to ensure transparency and to explain to individuals:

- The types of personal data we collect about individuals.
- How we collect personal data, why we need it and how we use it.
- The lawful basis we have for processing personal data.
- When and who do we share personal data with.
- How we secure personal data.
- How long we hold personal data for.
- Use of cookies, other technologies and the use of automated decision making and profiling.
- Individuals' legal rights in relation to personal data.
- How to contact us, including how to make a complaint with the supervisory authority.
- When the privacy notice was last updated.

5.8.1.2. UK GDPR Article 5(1)(e) - Storage Limitation

UK GDPR Article **5(1)(e)** specifies that Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Personal Data may be stored for longer periods to the extent as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article **89(1)** subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

5.8.1.3. Periodic review of Personal Data

Personal Data processed by HEIW must be reviewed regularly and if it is no longer required shall be securely destroyed or anonymised as appropriate.

5.8.1.4. Challenges to the retention of Personal Data

Under Article **17** of the UK GDPR, individuals have the right to have personal data erased. Any challenges made in relation to the retention of Personal Data shall be considered in accordance with UK GPPR Article 17 - Right to erasure ('right to be forgotten'). The right to erasure however might not apply where HEIW is legally obliged to process Personal Data or where the processing of Personal Data is required for HEIW to perform its functions. In such cases where Personal Data cannot be erased, HEIW must implement procedures to restrict the processing of Personal Data.

5.8.1.5. Audit, legal matters or investigation

Processes must be in place to ensure that records pending audit, legal process and/or investigation are not destroyed.

5.8.2. Welsh Government Records Management Code of Practice

To ensure the consistent retention of records and the information they contain throughout their lifecycle, HEIW has adopted the Welsh Government (WG) NHS Records Management Code of Practice for Health and Social Care 2022. Specific requirements relating to record retention are expressed in **Appendix A**.

5.9. Disposal

Records in any format should not be kept beyond their designated retention period or useful life. Once the retention period or useful life of a record has been reached, the record will need to be appropriately reviewed. Under review, a decision shall be taken to either securely destroy the record or retain the record because the record is still required by HEIW.

5.9.1. Records Destruction

The destruction of records can take many forms, from a simple delete of electronic information to permanent destruction using physical or technology mechanisms.

Destruction of records and the information they contain must be completed in a defendable way to ensure that information in destroyed appropriately and where required in a controlled, compliant, and legally defensible way. The destruction of records must be authorised and signed-off by an appropriate individual and in line with HEIW's legal obligations.

Physical records containing information must be destroyed appropriately, such as being placed in the blue confidential waste bins located throughout Ty Dysgu. Electronic records and the information they contain must be destroyed accordingly and in line with relevant security policies.

The nature, requirements and methods of destruction will be determined by the record type, its format, and the information it contains.

Decisions to destroy records shall be recorded to maintain an audit trail. Where records and the information they contain are destroyed, a record of destruction must be recorded and appropriately stored. Information Asset entries recorded on the Information Asset Register (IAR) must be updated accordingly.

5.9.2. Retaining Records

In certain circumstances, HEIW may be required to retain records beyond the established retention period. This may pertain to records necessary for an upcoming audit, legal proceedings, or investigations.

In such cases where records are still required, a new retention period shall be defined. Information Asset entries recorded on the Information Asset Register (IAR) must be updated accordingly.

6. Definitions

6.1. Record

The ISO standard ISO 15489-1:2016 defines a record as:

Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business.

6.2. Document

A document is any piece of written matter in any form, produced or received that provides information or evidence or serves as a record.

6.3. Personal Data

Personal Data has its meaning given to it in Data Protection Legislation:

"**Personal Data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

6.4. Special Category Data

Some personal data can be more sensitive in nature and thus requires a higher degree of protection. The UK GDPR defines this type of data as 'special category data' which include:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions.
- Personal data revealing religious or philosophical beliefs.
- Personal data revealing trade union membership.

- Genetic data.
- Biometric data (where used for identification purposes).
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.

6.5. Processing

Processing in relation to personal data means the operations which are performed on personal data (this includes automated means) such as the collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

6.6. Lawful Basis for Processing Personal Data

The lawful basis for the processing of personal data is set out in Article 6.1 of the UK GDPR. At least one of the lawful basis for processing personal data must apply when processing personal data:

a) **Consent:** the individual has given clear consent for you to process their Personal Data for a specific purpose.
b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's Personal Data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Where Special Category Data us processed, there are 9 conditions for processing set out in Article **9.2** of the UK GDPR, these include:

a) Explicit consent.
b) Employment, social security, and social protection (if authorised by law).
c) Vital interests.
d) Not-for-profit bodies.
e) Made public by the data subject.
f) Legal claims or judicial acts.
g) Reasons of substantial public interest (with a basis in law).

h) Health or social care (with a basis in law).
i) Public health (with a basis in law).
j) Archiving, research, and statistics (with a basis in law).

If an organisation is relying on conditions **(b)**, **(h)**, **(i)** or **(j)**, they will also need to meet the associated condition in UK law, set out in **Part 1 of Schedule 1** of the DPA 2018.

If an organisation is relying on the substantial public interest condition set out in Article **9(2)(g)**, they will need to meet one of **23** substantial public interest conditions detailed in **Part 2 of Schedule 1** of the DPA 2018.

6.7. Individual Rights

Individuals have the right to be informed about the collection and use of their personal data and about the processing of their personal data. These rights include:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restricted processing
- Right to data portability
- Right to object
- Rights related to automated decision-making including profiling

6.8. Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help identify, assess, and manage data protection and privacy risks which are associated with a project or plan. DPIA's are an essential part of HEIW's accountability obligations under the UK GDPR and carrying out a DPIA is a legal requirement for any type of personal data processing, including processing that is likely to result in a high risk to individuals rights and freedoms.

6.9. Information Asset

An Information Asset is considered a body of information (electronic or physical) managed as a single unit so it can be understood, valued, classified, inventoried, protected, managed, and used effectively.

6.10. Information Asset Register

An Information Asset Register (IAR) a record of the information assets which are created, owned, and managed by HEIW.

7. Equality Impact Assessment

After seeking pertinent advice from HEIW's Equality, Diversity and Inclusion team, it was agreed the content of this policy is mandatory and outlines HEIW's legal and organisational responsibilities in respect of appropriate records management. This Policy and procedures underpinning and supporting the implementation of this policy shall be assessed against accessibility and usability to ensure they do not have a negative impact on individuals with protected characteristics.

8. Awareness and Training

HEIW will ensure that adequate training is provided to all staff involved in the processing of Personal Data and that qualified expertise is available for consultation.

All new starters shall undertake mandatory ESR information governance, records management, and cyber security training as part of the HEIW induction process.

All staff shall undertake mandatory ESR information governance, records management, and cyber security training every two years.

All staff who require support in understanding the legal, professional, and ethical obligations that apply to them should contact the Information Governance team.

9. References

Links to the Information Commissioners Office (ICO) provide a valuable source of information:

The ICO recommends that all public authorities should be aware of the Secretary of State's Code of Practice on records management:

- ICO Records Management and Security

Welsh Government (WG) Records Management Code of Practice for Health and Social Care 2022:

- Records Management Code of Practice for Health and Social Care 2022

10. Getting Help

For further advice or assistance on how to ensure compliance with this policy, please contact the Information Governance team.

Information Governance team: HEIW.InformationGovernance@wales.nhs.uk

11. Legislation and Standards

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000 (FOIA)
- Public Records Acts 1958 / 1967 (PRA)

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

- Caldicott Principles
- Information Security: ISO/IEC 27001
- Information Commissioners Codes of Practice
- NHS England Records Management Code of Practice 2021 (formally NHSX)
- Welsh Government Records Management Code of Practice for Health and Social Care 2022

Other references include:

- Privacy and Electronic Communications Regulations 2003
- Computer Misuse Act 1990
- Copyrights, Designs & Patents Act
- Human Rights Act 1998
- Fraud Act 2006
- The Regulation of Investigatory Powers Act 2000
- Common Law - Duty of Confidence
- Information Governance Assurance Programme Guidance 2008-9
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Caldicott Report 2013
- Professional Codes of Conduct

12. Related Policies and Procedures

This policy should be read in conjunction with the following policies and procedures:

- All Wales Information Governance Policy
- All Wales Information Security Policy
- All Wales Email Use Policy
- All Wales Internet Use Policy
- All Wales Social Media Policy
- Data Protection and Confidentiality Policy
- Breach Reporting Procedure
- Information Asset Procedure
- Subject Access Request Procedure
- Freedom of Information Act Policy

13. Publication and Dissemination of Organisation Wide Documents

The Board Secretary is responsible for publishing email notices regarding newly approved organisation-wide documents.

The Senior Management team is responsible for notifying staff of the document's publication and ensuring they have access to such documents so that they can be implemented as necessary by staff in their daily role.

14. Compliance

Guidance on the policies and procedures necessary to comply with this policy will be made available to all staff. Managers will be responsible for ensuring that all their staff are made aware of HEIW policies, procedures, and work instructions.

HEIW trusts its workforce, however it reserves the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that the employee practices in work may come under scrutiny. HEIW respects the privacy of its workforce and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

Staff should be reassured that HEIW takes 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 of a policy or legislation breach. Furthermore, on deciding

whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the member of staff.

Managers are expected to speak to staff of their concerns should any minor issues arise. If breaches of information governance policies are detected an investigation may take place. Where information governance policies are found to have been breached, disciplinary procedures may be followed. Concerns about possible fraud and/or corruption should be reported to the Counter Fraud team.

In order for HEIW to achieve effective and good information governance, all staff must be encouraged to recognise the importance of information governance and report any data breaches or issues (including suspected breaches) to enable lessons learned.

Staff 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 practices. This should minimise the risk of incidents and breaches occurring or recurring.

15. Policy Review

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

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

Appendix A

Welsh Governments (WG) NHS Records Management Code of Practice for Health and Social Care 2022. Under the Public Records Act (PRA), public bodies are required to identify records of historical value and transfer them to a PoD by the time they are 20 years old.

In most cases Welsh bodies will transfer their records to a PoD such as the local archive or the National Library of Wales. If the record has potential historical or social value, then consider retaining for longer than the original retention period. It would also be helpful to have early discussions with the local PoD about potential accession, even if the record has ceased to be of operational value or use. PoDs will not normally accession records before 20 years retention has passed, unless there are exceptional circumstances for early transfer.

Retention Requirements:

Staff / Trainee Records:

Record Type	Retention Period	Disposal Action	Notes
Staff record.	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner.	Review and consider transfer to PoD.	This includes, but is not limited to, evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms.
Staff record: summary.	Keep until 75th birthday.	Review and consider transfer to PoD.	Please see the good practice box staff record summary used by an organisation. Some organisations create summaries after a period since the staff member left (usually 6 years). This practice is ok to continue if this is what currently occurs.
Trainee personnel records	6 years.	Review, anonymise or destroy if no longer required.	This includes, but is not limited to, qualifications, experience, evidence of right to work, security checks and recruitment documentation for the appropriate courses.

Appraisal records.	6 years.	Review, anonymise or destroy if no longer required.	Retention begins from the date of meeting.
Recruitment records - Successful candidates.	Length of Employment, plus 1 year.	Review, anonymise or destroy if no longer required.	Retention begins from the date of employment.
Recruitment records - Unsuccessful Candidates.	Minimum 6 months. Maximum 12 months.	Review, anonymise or destroy if no longer required.	Court action can only be actioned within the initial 3 months.
Recorded conversations: which may be needed later for clinical negligence or other legal purposes*.	6 years.	Review and destroy if no longer required.	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980.
Occupational health reports.	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner.	Review and destroy if no longer required.	Retention period runs from the date of the referral.
Occupational health report of staff member under health surveillance.	Keep until 75th birthday.	Review and destroy if no longer required.	Retention period runs from the date of the referral.
Timesheets (original record).	2 Years.	Review and destroy if no longer required.	This applies to all workforce timesheets.
Disciplinary records.	6 Years	Review and destroy if no longer required	Retention begins once the case is heard, and any appeal process completed. The record may be retained for longer, but this will be a local decision based on the facts of the case. The more serious the case, the more likely it will attract a longer retention period. Likewise, a one-off incident may need to only be kept for the minimum time stated. This applies to all cases, regardless of format.

Training Records:

Record Type	Retention Period	Disposal Action	Notes
Clinical Training records - Statutory training for role.	75th Birthday or 6 years after leaving.	Review, anonymise or destroy if no longer required.	e.g., Medical related training.
Mandatory training records.	10 years.	Review, anonymise or destroy if no longer required.	e.g., ESR Training for NHS Wales Staff.
Attendance records.	1 year.	Review, anonymise or destroy if no longer required.	Attendance to events, informal training or awareness sessions.

Corporate Governance Records:

Record Type	Retention Period	Disposal Action	Notes
Board meetings*.	Up to 20 years.	Review and transfer to PoD.	A local decision can be made on how long to retain the minutes of board meetings, and associated papers linked to the board meeting, but this must not exceed 20 years, and will be required to be transferred to The National Archives for National Bodies.
Board meetings: closed boards*.	Up to 20 years.	Review and transfer to PoD.	Although these may still contain confidential or sensitive material, they are still a public record and must be transferred at 20 years, and any FOI exemptions noted, or indications that the duty of confidentiality applies.
Chief Executive records*.	Up to 20 years.	Review and transfer to PoD.	This may include emails and correspondence where they are not already included in board papers.
Committees: major, listed in Scheme of delegation or report direct into the board,	Up to 20 years.	Review and transfer to PoD.	Includes high level meetings, major projects, and departmental business meetings. These may have local historical value required transfer consideration.
Committees: minor, not listed in scheme of delegation*.	6 years.	Review and consider transfer to PoD.	Includes minor meetings, projects, and departmental business meetings. These may have local historical value required transfer consideration.
Data Protection Impact Assessments (DPIAs).	6 years.	Review and destroy if no longer required.	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one-off, then 6 years from completion.
Destruction certificates or records held on physical media.	20 years.	Review and dispose of if no longer required.	Consideration should be given to a selection of these as an indicator of what has not been preserved.
Electronic metadata destruction stubs.	20 years.	Review and destroy if no longer required.	Refer to destruction certificates.
Incidents: serious.	20 years.	Review and consider transfer to PoD.	Retention begins from the date of the Incident; not when the incident was reported.

Incidents: not serious.	10 years.	Review and destroy if no longer required.	Retention begins from the date of the incident; not when the incident was reported.
Incidents: serious incidents requiring investigation.	20 years.	Review and consider transfer to PoD.	These include independent investigations into incidents. These may have permanent retention value. If they are not required, then destroy.
Non-clinical QA records.	12 years.	Review and destroy if no longer required.	Retention begins from the end of the year to which the assurance relates.
Policies, strategies and operating procedures, including business plans*.	Life of organisation plus 6 years.	Review and consider transfer to PoD.	Retention begins from when the document is approved, until superseded. If the retention period reaches 20 years from the date of approval.
Quarterly reviews from NHS	Quarterly reviews from NHS	Quarterly reviews from NHS.	Quarterly reviews from NHS.
Risk registers.	6 years.	Review and destroy if no longer required.	Retention period in accordance with the Limitation Act and corporate awareness of risks.
Staff surveys: individual returns and analysis.	1 year after return.	Review and destroy if no longer required.	Forms are anonymous so do not contain PID unless provided in free text boxes.
Staff surveys: final report.	10 years.	Review and consider transfer to PoD.	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
Trust submission forms.	6 years.	Review and destroy if no longer required.	Trust submission forms. 6 years. Review and destroy if no

Finance & Procurement Records:

Record Type	Retention Period	Disposal Action	Notes
Financial transaction records.	6 years.	Starting from the financial year they relate to.	This period can be extended, provided there is justification and organisational approval.
Invoices.	6 years.	Starting from the financial year they relate to.	Invoices that have been paid by HEIW or on behalf of HEIW
Tenders (successful or not).	6 years.	Review and destroy if no longer required.	This period can be extended, provided there is justification and organisational approval.
Contracts sealed or unsealed.	Retain for 6 years after the end of the contract.	Review and destroy if no longer required.	This period can be extended, provided there is justification and organisational approval.
Contracts - financial approval files.	Retain for 15 years after the end of the contract.	Review and destroy if no longer required.	This period can be extended, provided there is justification and organisational approval.
Contracts - financial approved suppliers' documentation.	Retain for 11 years after the end of the contract.	Review and destroy if no longer required.	This period can be extended, provided there is justification and organisational approval.
Accounts.	3 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate. Includes all associated documentation and records for the purpose of audit.
Final annual accounts report*.	Up to 20 years.	Review and transfer to PoD.	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with board papers for that year to keep a complete set of governance papers.
Benefactions.	8 years.	Review and consider transfer to PoD.	These may already be in the financial accounts and may be captured in other reports, records or committee papers.
Debtors' records: CLEARED.	2 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.
Debtors' records: NOT CLEARED.	6 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.
Donations.	6 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.

Expenses.	6 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.
Petty cash.	2 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.
Private Finance Initiatives (PFI) files.	Lifetime of PFI.	Review and consider transfer to PoD.	Retention begins at the CLOSE of the financial year to which they relate.
Staff salary information or files.	10 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.
Superannuation records.	10 years.	Review and destroy if no longer required.	Retention begins at the CLOSE of the financial year to which they relate.

Communications & Engagement Records:

Record Type	Retention Period	Disposal Action	Notes
Intranet site.	6 years.	Review and consider transfer to PoD.	This period can be extended, provided there is justification and organisational approval.
Patient information leaflets.	6 years.	Review and consider transfer to PoD.	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.
Press releases and important internal communications.	6 years.	Review and consider transfer to PoD.	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.
Public consultations.	5 years.	Review and consider transfer to PoD.	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation, particularly where this resulted in changes to the services provided and so may have historical value.
Website.	6 years.	Review and consider transfer to PoD.	This period can be extended, provided there is justification and organisational approval.
Photographic collections: service locations, events and activities.	Up to 20 years.	Review and consider transfer to PoD.	These provide a visual historical legacy of the running and operation of an organisation. They may also provide secondary uses, such as use in public inquiries.

Legal, Complaints & Information Rights Records:

Record Type	Retention Period	Disposal Action	Notes
Complaints Case files.	10 years	This period can be extended.	Initial complaint, meeting notes and documentation and any subsequent administration undertaken.
Fraud: case files.	6 years.	Review and destroy if no longer required.	Retention begins at the CLOSURE of the case. This also includes cases that are both proven and unproven.
FOI requests.	3 years.	Review and destroy if no longer required.	Retention begins from the date of request.
FOI appeals.	6 years.	Review and destroy if no longer required.	Retention begins from the date of request.
SAR (all correspondence).	3 years.	Review and destroy if no longer required.	Retention begins from the date of request.
SAR appeals.	6 years.	Review and destroy if no longer required.	Retention begins from the date of request.
Industrial relations: including tribunal case records.	10 years.	Review and consider transfer to PoD.	Retention begins at the CLOSE of the financial year to which it relates. Some organisations may record these as part of the staff record, but in most cases, they should form a distinctive separate record
Litigation records.	10 years.	Review and consider transfer to PoD.	Retention begins at the CLOSURE of the case.
Intel patents, trademarks, copyright, IP.	Lifetime of patent, or 6 years from end of licence or action.	Review and consider transfer to PoD.	Retention begins at the END of lifetime or patent, or TERMINATION of licence or action.
Software licences.	Lifetime of software.	Review and destroy if no longer required.	Retention begins at the END of lifetime of software.

Facilities & Compliance Records:

Record Type	Retention Period	Disposal Action	Notes
Physical access control system logs.	Between 30 and 90 days.	Review and destroy if no longer required	Retention period is for security monitoring only. This period can be extended, provided there is justification and organisational approval.
Building plans, including records of major building works.	Lifetime (or disposal) of building plus 6 years.	Review and destroy if no longer required.	Building plans and records of works are potentially of historical interest and where possible, should be kept.
Surveys: building or installation, not patient surveys.	Lifetime of installation or building.	Review and destroy if no longer required.	Retention period begins at the END of INSTALLATION period.
Leases.	12 years.	Review and destroy if no longer required	Retention begins at point of lease termination.
Closed Circuit Television (CCTV)	Between 30 and 90 days.	Review and destroy if no longer required.	Retention period is for security monitoring only. This period can be extended, provided there is justification and organisational approval.
Equipment monitoring: general testing and maintenance work.	Lifetime of installation.	Review and destroy if no longer required.	Retention begins from the completion of the testing and maintenance.
Equipment maintenance logs.	11 Years.	Review and destroy if no longer required.	Retention begins from the completion of the testing and maintenance.

Other Relevant Records:

Record Type	Retention Period	Disposal Action	Notes
Advanced medical therapy Research: master file.	20 years.	Review and destroy if no longer required.	The sponsor of the study will be the primary holder of the study file and associated data.
Research: datasets.	No longer than 20 years.	Review and destroy if no longer required.	The sponsor of the study will be the primary holder of the study file and associated data.
Stakeholder records.	1 year.	Review, anonymise or destroy if no longer required.	HEI, Placement, Private Practises or any organisation that engage with HEIW
Engagement notes / meeting minutes.	Up to 6 years - content will determine retention period.	Review, anonymise or destroy if no longer required.	This could be for routine staff meetings or project-based meetings.