



Gwasanaeth Cefnogi
Swyddog Diogelu Data
Data Protection Officer
Support Service

IGDC • DHCW

Records Management Policy

Approved by: Mr Alex Davies

Version: Version 2026,5.0

Last Updated: 10/03/2026

Review date: 10/03/2027

TABLE OF CONTENTS

Document history	2
1.1 Revision history	2
1.2 Reviewers	2
1.3 Authorisation	2
2 Introduction	3
3 Scope.....	3
3.1 Legislative Compliance	3
4 Policy Objectives.....	4
5 Roles and Responsibilities	4
5.1 Senior Responsible Person	4
5.2 Information Governance Lead	4
5.3 Data Protection Officer.....	4
5.4 Caldicott Guardian	5
5.5 All Staff.....	5
6 Policy Framework	5
6.1 What is a record?	5
6.2 Standards.....	6
6.3 Creating Records.....	7
6.4 Organising Records.....	7
6.5 Information Asset Register (IAR)	7
6.6 Off – Site Storage	7
6.7 Security and Access.....	8
6.8 Retention.....	8
6.9 Disposal.....	9
6.10 Reappraisal.....	9
6.11 Permanent Preservation.....	9
6.12 Destruction.....	10
6.13 Information not listed on the Records Retention Schedule.....	10
7 Review.....	10



Document history

1.1 Revision history

Date	Version	Author	Revision Summary
10/03/2026	2026,5.0	Mr Alex Davies	This policy has been based upon Version 5.0 of the DPO Support Service Template

1.2 Reviewers

This document requires the following reviews:

Date	Version	Name	Position

1.3 Authorisation

Signing of this document indicates acceptance of its contents.

Approver's Name:	Caldicott Guardian
Role:	GP Partner
Signature:	 <hr/> <p>Dr Maria Vincent GP Partner Caldicott Guardian 10/03/2026</p>



2 Introduction

This policy has been developed for use by The Vale Of Neath Practice in line with the [Welsh Records Management Code of Practice for Health and Social Care 2022](#) and the current regulatory and legal framework. Compliance with this policy will help to ensure the organisation is compliant with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and the [Code of Practice on the management of records issued under S46 of the Freedom of Information Act 2000](#).

Records management is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources of the organisation. It is of paramount importance to ensure that records are efficiently managed, this policy sets out the way that the organisation will retain, process, and dispose of records.

The organisation recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The organisation is committed to ensuring accurate, timely and relevant records management, as is essential to deliver the highest quality healthcare. As such, it is the responsibility of all organisation staff to ensure that the record keeping standards outlined in this policy, and the subsequent retention periods of records are adhered to.

3 Scope

This policy applies to all staff of The Vale Of Neath Practice.

The term 'staff' includes all health professionals, partners, staff members, locums, students, trainees, secondees, volunteers, contracted third parties and any persons undertaking duties on behalf of The Vale Of Neath Practice.

This policy applies to all records created, received, maintained, and held, in all formats, by staff of the organisation in the course of carrying out their functions. Records are defined as documents, regardless of format, which facilitate the operations and business of the organisation, and which are thereafter retained for a set period to provide evidence of its activities and transactions, as detailed within the Retention Schedule.

This policy applies to all employees of the organisation, including associates, contractors, temporary staff and any students who are carrying out work on behalf of the organisation.

This policy should be read in conjunction and reviewed in-line with the following:

Information Governance Policy

Information Security Policy

Data Quality Policy

Breaches of this policy will be reported via the organisation's incident reporting processes and dealt with in line with the organisation's Disciplinary Policy where appropriate. organisation

3.1 Legislative Compliance

The management of records held by the organisation is regulated by the following regulatory frameworks:

- [Data Protection Act 2018 & UK General Data Protection Regulation \(UK GDPR\)](#)
- [Freedom of Information Act 2000](#)
- [Health and Social Care Act 2008](#)
- [Caldicott Principles](#)
- [Limitation Act 1980](#)



- [Consumer Protection Act 1987](#)
- [Welsh Health Circular \(WHC\) \(99\)7](#)
- [Public Records Act 1958](#)
- [Local Government \(Wales\) Act 1994](#)
- [Code of Practice on the management of records issued under S46 of the Freedom of Information Act 2000.](#)

4 Policy Objectives

This policy:

- Sets the standard for the management of records to meet the business needs at The Vale Of Neath Practice.
- Ensures compliance with legislation, regulations, and standards
- Outlines accountability and responsibilities

5 Roles and Responsibilities

5.1 Senior Responsible Person

The Senior Responsible Person within the organisation is responsible for ensuring the highest level of organisational commitment to this policy and the availability of resources to support its implementation. Where appropriate, the Senior Responsible Person may delegate specific responsibilities to other individuals who have responsibility for information governance within the organisation.

The Senior Responsible Person will ensure that all staff are aware of this policy, understand their responsibilities in complying with the requirements of this policy and are up to date with mandatory information governance training.

Additionally, the Senior Responsible Person will ensure the key roles outlined below are established within the organisation's management structure.

The Senior Responsible Person within The Vale Of Neath Practice is Caldicott Guardian.

5.2 Information Governance Lead

The Information Governance (IG) Lead is responsible for liaising with and supporting the Data Protection Officer and Caldicott Guardian in coordinating and implementing the confidentiality and data protection work programme within the organisation.

Where necessary, the IG Lead will supervise and direct the work of others to aid the organisation in meeting its information governance responsibilities.

The IG Lead will act as the first point of contact for information governance queries within the organisation.

The Information Governance Lead within The Vale Of Neath Practice is Caldicott Guardian.

5.3 Data Protection Officer

The Data Protection Officer (DPO) provides independent risk-based advice to support the organisation in its decision making in the appropriateness of processing personal and special categories of data within the Principles and Data Subject Rights laid down in the UK General Data Protection Regulation (UK GDPR).



The DPO role is to 'inform and advise' and not 'to do', they are a trusted advisor whom the organisation should actively seek advice from.

The Data Protection Officer for The Vale Of Neath Practice is the Digital Health and Care Wales (DHCW) Data Protection Officer Support Service.

The DPO can be contacted by emailing DPOService@wales.nhs.uk.

5.4 Caldicott Guardian

The Caldicott Guardian has responsibility for ensuring that patient information is used legally, ethically, and appropriately, and that confidentiality is always maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

The Caldicott Guardian will apply the eight principles and act as "the conscience of the organisation" regarding information sharing.

The Caldicott Guardian within The Vale Of Neath Practice is Dr Maria Vincent.

5.5 All Staff

All staff have a responsibility for information governance and maintaining appropriate security for their own work area.

All staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. Mandatory information governance training must be undertaken at least every two years.

6 Policy Framework

6.1 What is a record?

The ISO standard; ISO 15489-1:2016 Information and documentation - Records management, defines a record as '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.'

Examples of records that should be managed using the guidelines in this policy are listed below. This list gives examples of functional areas as well as the format of the records:

Function:

- Patient health records (electronic or paper based, including those concerning all specialties and GP records)
- Pharmacy prescription records
- Records of private patients seen on NHS premises
- Accident & emergency, birth, controlled drugs and all other registers
- Theatre registers and minor operations (and other related) registers
- Administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling)
- X-ray and imaging reports, output and images
- Integrated health and social care records



- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.

Format:

- Photographs, slides, and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc
- E-mails
- Digital records
- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient)
- Websites and intranet sites that provide key information to patients and staff.

6.2 Standards

The following standards need to be maintained at all times:

- Records must be managed in a manner complying fully with legislative and regulatory requirements affecting their use and retention.
- Records must have relevant content, context and format, and must be accurate authentic, useable, reliable, timely and well managed.
- Records must directly relate to and support a service, function or activity delivered by the organisation and be able to support decision making.
- Records must serve the interests of the organisation, its staff, patients and other stakeholders by maintaining high quality documentation for appropriate lengths of time.
- Records must be managed via systems and processes ensuring efficiency and consistency throughout their lifecycle of creation, distribution, use, maintenance and disposal.
- Records must be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities.
- Records must be kept securely to ensure the confidentiality and importance of the content, being protected from unauthorised or unlawful disclosure.
- Records must be accessible and retrievable to support the continuity of organisation business and the efficiency of the provided services.
- Records must be retained and disposed of in compliance with the organisation's retention schedule.
- Records must undergo a review at the end of their retention period and, if no longer required, be securely destroyed in an efficient, timely and confidential manner.



6.3 Creating Records

All records must be accurate and complete, so that it is possible to establish what has been done and why. The quality of all records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met.

Where appropriate, templates should be used so that documents are produced consistently and can be stored in a cohesive manner. In addition to this, version control procedures should be used for drafting and revising documents, so that staff can easily differentiate between versions and readily identify the latest copy.

Both paper and electronic record systems should contain metadata to enable the records to be understood and stored/accessed easier.

6.4 Organising Records

Records should be organised and described in a uniform, logical manner that facilitates fast, accurate and comprehensive retrieval so that they are easily accessible when they are required.

Classifying records and holding them in an appropriate filing structure will enable suitable retention periods to be assigned. Keeping diverse records together in a less structured format will make it difficult to identify and retrieve records when they are needed and make it difficult to assign retention periods.

Digital storage of records enables records to be tagged and introduces a searching functionality which can be used to locate records quickly.

Any duplicate records that are retained increases the risk regarding the management use and alteration of the record. There may be need to keep a local version of a record centrally, however, it should be avoided where possible and a system enabling the use of a single central version implemented.

Where possible, to reduce the need for duplication of documents, records should be stored in central folders that are accessible to relevant staff. Digital records should be stored in a shared workspace whenever possible. Titles of these digital records should be easily identifiable and agreed naming conventions used.

6.5 Information Asset Register (IAR)

The organisation must identify and appoint an individual to fulfil the role of an Information Asset Owner (IAO) to take responsibility of individual records or record sets.

The organisation will maintain an up to date Information Asset Register (IAR) that records assets, systems and applications used for processing or storing personal data across the organisation.

The IAR will support information access, ensuring that the organisation can locate information about past activities in a timely manner and enabling the more effective use of resources.

The IAR holds information such as asset location and retention periods relating to personal information and corporate information which is reviewed periodically to ensure it remains up to date and accurate.

6.6 Off – Site Storage

When storage of physical records is unavailable, the organisation may use a contracted off-site storage provider, The Maltings Document Storage Solutions Limited, East Tyndall Street, Cardiff.



Regular due diligence checks will be undertaken to ensure records stored off-site are done so securely. Records stored off-site need to be considered carefully as it will take longer to recall the records to the organisation in the event that they are needed.

6.7 Security and Access

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with the organisation's Information Governance policy. Records must be stored in safe and secure physical and digital environments, taking account of the need to preserve important information in a useable format enabling ease of access in correlation to the frequency of use.

Records should be stored in a centralised storage or filing system or on a shared drive, so that departments can operate efficiently when individual members of staff are absent. Where appropriate, access to central records should be appropriately available across the organisation in order to avoid recreating information that already exists and storing duplicate data unnecessarily.

Records that would be vital to the continued functioning of the organisation in the event of a disaster must be identified and protected. These include records that would recreate the organisation's legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders. All critical business data must be protected by appropriate preservation, backup and disaster recovery policies. Where vital records are only available in paper format it is best practice that they are duplicated, and the originals and copies stored in separate locations. If duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect vital documents.

6.8 Retention

Records must only be kept for as long as is required to meet operational, business and legal needs. It is a legal requirement established by the DPA to only retain records containing personal data for as long as strictly necessary, and organisations can be subject to enforcement action by regulatory bodies, such as the ICO, for failing to comply.

The organisation has adopted the retention schedule set out in Appendix II of the [Records Management Code of Practice for Health and Social Care 2022](#).

The retention schedule is intended to provide guidance to all areas of the organisation regarding appropriate retention periods for the different categories of records held by the organisation. It applies to all formats of records and is intended to promote consistency and the retention of the minimum volume of records while accounting for requirements imposed by legislation and regulation.

Retention can be complicated if records of a dissimilar nature, with different retention requirements, are filed together. The organisation should consider retention periods when designing their records storage systems and practices to avoid this issue. Files should be reviewed regularly to ensure records are not kept for too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

The retention schedule includes the following information:

- **Record type** – The type of record or information asset, applying to all formats of record
- **Retention period** – The recommended length of time for which the records should be kept by the organisation
- **Disposal action** – This is the action that should be taken once the retention period has reached its end
- **Notes** – Any additional information unrelated to the three prior fields



6.9 Disposal

When a record reaches the end of its retention period, a review must be taken on the documents future. The outcomes of this review can be any of the following:

- Reappraisal
- Permanent preservation
- Destruction

6.10 Reappraisal

Before action is taken to permanently preserve or destroy a record at the end of its retention period, a reappraisal of any need to retain it for present functions should be undertaken, it should only be necessary to revise the retention period on rare occasions.

In some circumstances it may be necessary to retain a record for longer than its defined retention period. A new operational function requiring its retention may have arisen, or it may be required for investigation or litigation purposes, or because it is needed in order to respond to an access request received under data protection or freedom of information legislation. If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision while taking circumstances into account. A period of one year is recommended.

The DPA and FOI Act contain provisions relating to the destruction or alteration of information or records after a legal access request has been received. Such destruction or alteration will be considered a disciplinary offence. FOI Act also creates a criminal offence in relation to these actions.

Examples of when information may be required to be held for longer periods are where:

- The information is subject to a request for information under access to information legislation such as a Subject Access Request under the Data Protection Act or a request under the Freedom of Information Act
- The organisation is subject to ongoing legal action in which the information relates
- The information is subject to an investigation, for example the Infected Blood Inquiry
- There is a greater public interest in an issue requiring long term preservation of the information.

6.11 Permanent Preservation

Some of the organisation's records may be retained permanently as they have long term evidential or historical value. The organisation's retention schedule should help to identify records that have archival value. The following records are examples of items that may be worthy of permanent preservation:

- Records that document policy formation
- Records that show the development of the organisation and its infrastructure
- Records that show evidence of important decisions or precedent
- Records showing the development of the relationship between the organisation's staff and the organisation's corporate functions
- Records documenting the organisation's relationship with external parties and stakeholders, and the organisation's place in the local, national and international community.

Where records are considered to be of historical value the organisation should contact a local place of deposit who will assess and transfer the appropriate records for preservation.



6.12 Destruction

The destruction of records is an irreversible act which must be clearly documented and carefully considered. All records identified for disposal will be destroyed under confidential conditions in accordance with the organisation's retention schedule.

A decision for destruction must be made by the Caldicott Guardian. Measures such as certificates of destruction are to be requested by the organisation to ensure personal data is destroyed confidentially and a trusted suppliers is used with appropriate agreements in place outlining their responsibilities. A destruction log should be maintained.

Shred-It – Secure Document Destruction Services

When disposing of digital records, the organisation will ensure that all traces of the record are deleted securely, and are not duplicated on other systems, hard drives, servers or removable storage devices.

6.13 Information not listed on the Records Retention Schedule

Occasionally documents and information held by the organisation may not be specifically listed on the retention schedule. In such cases information should be held for the time of appropriate equivalent records, for example petty cash records should be retained in line with financial transaction records.

7 Review

This policy will be reviewed every 12 months or more frequently where the contents are affected by major internal or external changes such as:

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

