Gwasanaeth Cefnogi
Swyddog Diogelu Data
Data Protection Officer
Support Service
IGDC • DHCW

Data Quality Policy

Approved by: Mr Alex Davies

Version: 2026.3.0

Last Updated: 10/03/2026

Review date: 10/03/2027

TABLE OF CONTENTS

1. Document history

1.1 Revision history

Date	Version	Author	Revision Summary
10/03/2026	2026.3.0	Mr Alex Davies	This policy has been based upon Version 3.0 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:	 Dr Maria Vincent GP Partner Caldicott Guardian 10/03/2026

2. Introduction

This Data Quality Policy is The Vale Of Neath Practice policy for ensuring the accuracy of information which we store and process. Data quality is crucial, and the availability of complete, accurate, relevant and timely data is important in supporting patient care, governance, management and service agreements for health care planning and accountability.

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

- Records Management Procedure
- Individual Rights Procedure
- Information Governance Policy
- Information Sharing Procedure
- Information Security 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.

4. Policy Objectives

This policy covers all data which we process either in hardcopy or digital copy, including special categories of data. The aim of the policy is to ensure the availability of accurate and timely data which is vital for the safety of our patients and the safe and responsible running of our organisation.

The purpose of this policy is to provide general principles for the management of all data and guidance. This is to ensure that the organisation can take decisions based on accurate and complete data, and can meet its various legal and regulatory responsibilities. Information accuracy is a legal requirement under the UK GDPR and the Data Protection Act 2018. This policy provides the framework to mitigate against the risk of poor data quality and enable individuals within the organisation to take direct responsibility for any data they record.

5. Roles and Responsibilities

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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.

5.6. 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 General Guidelines and Data Quality Principles

Supplying accurate data is a complicated task for several reasons:

- There are many ways for the data to be inaccurate for example data entry errors and incomplete data.
- Data can be corrupted during translation depending on who is translating it, how and with what tools/processes.
- Data must relate to the correct time period and be available when required.
- Data must be in a form that is collectable, and which can subsequently be analysed.

To ensure an organisation achieves data quality, it must set out how:

- Data is collected and co-ordinated.
- Data is transferred between systems.
- Data is organised.
- Data is analysed.
- Data is interpreted.
- Conclusions and results drawn from the data are validated.

The following overarching principles underpin the approach to data quality:

- All staff will conform to legal and statutory requirements and recognised good practice, aim to be successful regarding in-house data quality indicators, and will strive towards 100% accuracy across all information systems.
- All data collection, manipulation and reporting processes by the organisation will be covered by clear procedures which are easily available to all relevant staff, and regularly reviewed and updated.
- All staff should be aware of the importance of good data quality and their own contribution to achieving it and should receive appropriate training in relation to data quality aspects of their work.
- Teams should have comprehensive procedures in place for identifying and correcting data errors, ensuring that information is accurate and reliable at time of use.

6.2. Ensuring accuracy

The Vale Of Neath Practice commits to ensuring that we comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 that we will “maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided”.

We ensure accuracy in our data in both hardcopy and digital records, by making sure all data has the following characteristics:

Authentic – the data is what it claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed.

Reliable – the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records.

Integrity – the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified.

Useable – the data can be located when it is required for use and its context is clear in a contemporaneous record.

Timely – the data is recorded as close as possible to being gathered and can be accessed easily, quickly and efficiently.

The principal purpose of service user records is to record and communicate information about the individual and their care. The principal purpose of staff records is to record employment details for payroll and business planning purposes.

To fulfil these purposes, we:

- Use standardised structures and layouts for the contents of records;
- Ensure documentation reflects the continuum of care, that all care is person centred and that care records are viewable in chronological order;
- Provide a clearly written care plan when care is being delivered by several members of the team, and we ensure that records are maintained and updated, and shared with everyone involved;
- Train staff on the creation and use of records (see staff handbook and the Record Management Policy) and provide training on good record keeping;
- Have implemented a procedure that enables service users and staff to have easy access to their records where appropriate. This is outlined in the Records Management Policy, Individual Rights Procedure, and our Privacy Notices.

All staff who record information, whether hardcopy or electronic, have a contractual responsibility to ensure that the data is accurate and as complete as possible. This responsibility extends to any system the staff member has access to.

6.3. Correction of errors

In-line with UK GDPR, individuals have the right to access to their personal data which we process and store. Patients have the right to the rectification of said records in the instance that their records are inaccurate or incomplete.

Where at all possible, in the instance that we have appropriately shared that individual's records with any third-party, we will inform this third-party of the rectification, if appropriate.

In all cases we will respond to a request for rectification within one calendar month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why an extension is required.

To request for their records to be rectified, service users or staff should contact us with the request for rectification either verbally or in writing. Individuals can submit a request to anyone within our organisation. Staff are aware of their responsibilities to pass on requests to the appropriate member of staff in a timely manner. If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.

While we are assessing the request to rectify records, we will restrict processing of the data in question. This will be done in line with our Individual Rights Procedure and Records Management Policy. In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received. A record of all rectification requests and outcomes will be logged on our Individual Rights Log.

All individuals who have their rectification request refused will be informed of their legal rights to complain to the Information Commissioner's Office (ICO) and to seek a judicial remedy.

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.