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

Information Security Policy

Approved by: Mr Alex Davies

Version: Version 2026,4.0

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	2026.4.0	Mr Alex Davies	This policy has been based upon Version 4.0 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 Policy has been developed in line with the All Wales Information Security Policy for Primary Care Service Providers.

The organisation will process a vast amount of information, held in a variety of formats. As data controller, the organisation is responsible for maintaining the security of this information.

The basic principles of information security that need to be maintained are:

- Confidentiality – The protection of information from unauthorised access
- Integrity – Safeguarding the accuracy and completeness of information and processes
- Availability – Ensuring that information is available to authorised people when needed

This policy does not restrict the organisation from sharing or disclosing information provided there is an appropriate legal basis for doing so. However, any information sharing which involves Personal Data or business sensitive information must be transferred securely.

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:

Information Governance Policy

Records Management 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.

4 Policy Objectives

The objective of this Policy is to set out how The Vale Of Neath Practice will maintain the security of the information it processes. This includes ensuring the organisation:

- Complies with the relevant legislation, including:
  - UK General Data Protection Regulation 2016
  - Data Protection Act 2018
  - Computer Misuse Act 1990
- Implements appropriate security controls for all business-critical manual and I.T. recording systems used within the organisation,
- Implements appropriate security measures that ensure the confidentiality, integrity and availability of information and I.T. systems,
- Makes staff aware of business continuity planning issues, and
- Makes all staff aware of the limits of their authority and their accountability.

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 Contracts of Employment

Staff security requirements will be addressed at the recruitment stage and all contracts of employment must contain an appropriate confidentiality clause. Information security expectations of staff is to be included within all job descriptions.

6.2 Security Control Assets

All ICT assets (hardware, software, applications or data) are to be allocated a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

In the event of loss or theft of an electronic portable device, the incident must be reported to the Caldicott Guardian and an incident report undertaken.

Users must not install any software on the working devices without prior authorisation and assessment by the Caldicott Guardian and the ICT provider.

6.3 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information. All staff have a responsibility to access only the information which they need 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.

6.3.1 Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.

Authorisation to use an application shall depend on the availability of a license from the supplier.

6.3.2 Physical Access Controls

The Vale Of Neath Practice is responsible for determining the security measures required based on local risk assessment. All staff are responsible for following these security measures and to ensure

they always maintain the confidentiality and security regardless of the setting (e.g. when working from home or working in the community).

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.

Where physical security measures exist, it must be ensured that they are employed at all times (e.g. filing cabinets must be locked, security doors and windows must be closed securely, blinds to secure areas closed). Access cards, PIN codes, keycodes, etc. must be kept secure and regularly changed as required.

All staff must ensure a clear desk and clear screen when away from their work area ensuring that confidential information, in any format, is secure and not visible to anyone who is not authorised to access it.

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.

6.3.3 Passwords

All staff are responsible for the security of their own passwords which must be developed in line with the Password Policy ensuring they are regularly changed. Passwords must not be disclosed to anyone, and users must not allow anyone to access any work devices, systems or applications using 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.

6.3.4 Remote Working

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. The Information Governance Risk Assessment for Offsite Working will be utilised to assess and manage risks involved on a case-by-case basis.

All staff of The Vale Of Neath Practice who use equipment outside of the organisation or NHS Wales premises, through the use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) are required to connect to the organisation's secure network and may only work remotely if a secure connection provided by The Vale Of Neath Practice or NHS Wales. For example, Virtual Private Network (VPN) tokens or MultiFactor Authentication (MFA) can be utilised as control measures. If the connection cannot be secured through these or an alternative approved by the Caldicott Guardian then remote working will not be permissible.

6.3.5 Staff Leavers and Movers

The Practice Manager 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 information, including access to confidential information, must not be transferred to a new role unless authorised by the Caldicott Guardian. The relevant checklist for leavers and movers must be completed in all cases.

6.3.6 Third Party Access to Systems

Any third-party access to systems must have prior authorisation, and where personal data is involved, authorisation must also be sought from the Practice Manager.

6.4 Storage of Information

All information stored on behalf of, or within The Vale Of Neath Practice is the responsibility of the organisation. All software, information and programmes developed for the organisation by the workforce during the course of their employment will remain the property of The Vale Of Neath Practice.

Staff are not permitted to use their personal devices or store confidential information on a personal device for the purpose of carrying out organisational business unless they have been explicitly authorised to do so in line with a documented organisational process (e.g. a Data Protection Impact Assessment).

All systems supported by the organisation will be backed up as part of their backup regime. Unless specifically told otherwise this will not include information held on local hard drives, portable devices or removable media. Users must not store information on local drives (usually referred to as the C Drive). Exceptions to this may be for legitimate work purpose to a device that is encrypted.

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 the Practice Manager.

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 the Practice Manager.

6.6 Transporting and relocation of information

6.6.1 Transporting Information

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

6.6.2 Relocating Information

When information, regardless of the format, is to be physically relocated to another location, local procedures must be formulated and followed by staff to ensure no information is left at the original location.

6.7 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of The Vale Of Neath Practice

6.8 Information Security Events and Weaknesses

All The Vale Of Neath Practice information security events, near misses, and suspected weaknesses are to be reported to the organisation's Data Protection Officer via DPOService@wales.nhs.uk and where appropriate reported as an adverse incident to the ICO within 72 hours of discovering the breach.

6.9 Portable Devices and Removable Media

Whilst it is recognised that both portable devices and removable media are widely used, 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, cameras and some forms of medical devices.

All portable devices must utilise appropriate technical measures to ensure the security of all data.

Users must not attach any personal (i.e. privately owned) portable devices to the organisations 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 information copied to removable media is encrypted.

6.10 Protection from Malicious Software

The organisation and its ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software.

All staff shall be expected to co-operate fully with this policy.

Staff shall not install software on the organisation's property without permission from the from the Practice Manager and the ICT Provider.

Users breaching this requirement may be subject to disciplinary action.

6.11 Business Continuity and Disaster Recovery Plans

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements).

A Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The Practice Manager has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

6.12 Requirements for New Processes, Services, Information Systems and Assets

The information governance requirements for new processes, services, information systems and assets must be complied with when a new process is to be established that involves processing of personal data (data relating to individuals) or changes are to be made to an existing process that involves the processing of personal data, this includes:

- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data.
- Introducing any new technology that uses or processes personal data in any way.

7 Training & Awareness

Information governance is everyone's responsibility. Training is mandatory for all staff providing NHS services and must be completed at commencement of employment and at least every two years subsequently.

Staff who need support in understanding the legal, professional and ethical obligations that apply to them should contact the Practice Manager as appropriate.

8 Monitoring System Access and Use

The Vale Of Neath Practice trusts its workforce; however, we reserve the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that staff practice in work may come under scrutiny. The Vale Of Neath Practice respect the privacy of their staff and do not want to interfere in their personal lives however, monitoring of work processes is a legitimate business interest.

Staff should be reassured that The Vale Of Neath Practice take a considered approach to monitoring; however, we reserve 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 appropriate Counter Fraud Team.

In order for The Vale Of Neath Practice to achieve good information governance practice, staff must be encouraged to recognise the importance of good governance and report any breaches to enable lessons 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 and at the right time. This should minimise the risk of incidents occurring or re-occurring.

9 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;
- Practice change or change in system/technology; or
- Changing methodology.