Cyngor Cymuned Ynysybwl & Coed Y Cwm Community Council

Data Protection Policy

1. Policy Statement

Ynysybwl & Coed Y Cwm Community Council is committed to protecting the privacy and security of personal data. We recognise the importance of handling personal information lawfully, fairly, and transparently, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy outlines the Council's commitment to data protection, detailing how we collect, store, process, and dispose of personal data, and ensuring that individuals' rights regarding their data are upheld. We aim to foster trust and confidence in our handling of personal information.

2. Scope

This policy applies to all personal data processed by Ynysybwl and Coed Y Cwm Community Council, regardless of its format (e.g., paper, electronic, audio, visual). It applies to all Councillors, employees, volunteers, contractors, and any third parties acting on behalf of the Council who handle personal data.

3. Definitions

- **Personal Data:** Any information relating to an identified or identifiable living individual (data subject). This includes, but is not limited to, names, addresses, email addresses, phone numbers, photographs, and IP addresses.
- **Special Category Data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. This data requires extra protection.
- **Processing:** Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **Data Subject:** The identified or identifiable living individual to whom the personal data relates.

- **Data Controller:** The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Ynysybwl and Coed Y Cwm Community Council is the Data Controller.
- **Data Processor:** A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.

4. Guiding Principles of Data Protection (UK GDPR)

The Council adheres to the seven key principles of data protection:

1. **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. **Purpose Limitation:** Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation:** Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy:** Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **Storage Limitation:** Personal data must 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 are processed.
6. **Integrity and Confidentiality (Security):** Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
7. **Accountability:** The Data Controller (Ynysybwl and Coed Y Cwm Community Council) is responsible for, and must be able to demonstrate compliance with, the other principles.

5. Roles and Responsibilities

- **The Community Council (as Data Controller):**
  - Has overall responsibility for compliance with UK GDPR and DPA 2018.
  - Ensures that appropriate technical and organisational measures are in place to protect personal data.
  - Approves this Data Protection Policy and ensures its effective implementation.
- **The Clerk to the Council:**
  - Acts as the primary point of contact for data protection queries and requests from data subjects.
  - Oversees the day-to-day implementation of this policy.
  - Maintains records of processing activities.
  - Provides advice and guidance to Councillors, employees, and volunteers on data protection matters.
  - Manages data breaches in accordance with this policy.
  - Liaises with the Information Commissioner's Office (ICO) if required.
- **All Councillors, Employees, and Volunteers:**
  - Must understand and adhere to this policy and associated procedures.
  - Are responsible for handling personal data securely and in accordance with training provided.
  - Must report any suspected data breaches or security incidents immediately to the Clerk.
  - Must not access, use, or disclose personal data without proper authorisation.

6. Lawful Basis for Processing Personal Data

The Council will only process personal data where it has a lawful basis to do so. The most common lawful bases for the Council's activities are:

- **Public Task:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council (e.g., providing local services, managing public spaces, responding to resident enquiries).
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which the Council is subject (e.g., payroll, financial reporting, statutory duties).

- **Contract:** Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g., employment contracts, service agreements).
- **Consent:** The data subject has given clear consent for the Council to process their personal data for a specific purpose. Consent will be freely given, specific, informed, and unambiguous, and easily withdrawn.

- **Legitimate Interests:** Processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. (Less common for public authorities but may apply in specific circumstances).

For **Special Category Data**, an additional condition for processing must be met, such as:

- Explicit consent.
- Processing necessary for employment, social security, or social protection law.
- Processing necessary for reasons of substantial public interest.
- Processing necessary for the establishment, exercise, or defence of legal claims.

7. Data Subject Rights

The Council respects the rights of individuals regarding their personal data. Data subjects have the following rights:

- **The Right to Be Informed:** Individuals have the right to be informed about the collection and use of their personal data. This is typically done through Privacy Notices.
- **The Right of Access:** Individuals have the right to request a copy of the personal data the Council holds about them (a Subject Access Request - SAR).
- **The Right to Rectification:** Individuals have the right to have inaccurate personal data rectified, or incomplete data completed.
- **The Right to Erasure (Right to be Forgotten):** Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

- **The Right to Restrict Processing:** Individuals have the right to 'block' or suppress the processing of their personal data in certain circumstances.
- **The Right to Data Portability:** Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- **The Right to Object:** Individuals have the right to object to processing based on legitimate interests or performance of a public task, direct marketing, or processing for purposes of scientific/historical research and statistics.
- **Rights in relation to automated decision-making and profiling:** Individuals have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning them or similarly significantly affects them.

All requests regarding data subject rights should be made in writing to the Clerk to the Council. The Council will respond to such requests within one calendar month.

8. Data Security

The Council will implement appropriate technical and organisational measures to ensure the security of personal data, protecting it from unauthorised or unlawful processing and against accidental loss, destruction, or damage. These measures include:

- **Physical Security:** Secure storage of paper records (e.g., locked cabinets).
- **IT Security:** Use of strong passwords, encryption where appropriate, firewalls, anti-virus software, and regular software updates.
- **Access Control:** Limiting access to personal data to only those who need it for their role.
- **Staff Training:** Ensuring all individuals handling data are aware of their responsibilities and security procedures.
- **Secure Disposal:** Ensuring personal data, whether paper or electronic, is securely disposed of when no longer needed.
- **Data Minimisation:** Only collecting and retaining data that is necessary.

9. Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

transmitted, stored, or otherwise processed.

- **Reporting:** Any suspected data breach must be reported immediately to the Clerk to the Council.
- **Investigation:** The Clerk will investigate the breach to determine its nature, scope, and impact.
- **Notification:** If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will notify the affected individuals and the Information Commissioner's Office (ICO) without undue delay, and no later than 72 hours after becoming aware of it.
- **Remedial Action:** The Council will take immediate steps to contain the breach, mitigate its effects, and prevent future occurrences.
- **Documentation:** All data breaches, regardless of severity, will be documented.

10. Data Retention

Personal data will not be kept for longer than is necessary for the purposes for which it was collected. The Council will establish and adhere to a Data Retention Schedule, which will specify the retention periods for different categories of personal data, based on legal, regulatory, and operational requirements.

11. Data Sharing

Personal data will only be shared with third parties where there is a lawful basis to do so and where appropriate safeguards are in place. This includes:

- **Data Processing Agreements:** Where a third party processes data on the Council's behalf (e.g., IT service providers, payroll providers), a written contract (Data Processing Agreement) will be in place, outlining their data protection obligations.
- **Secure Transfer:** Data will be transferred securely.
- **Necessity:** Data will only be shared when absolutely necessary for a specified purpose.

12. Training

All Councillors, employees, and volunteers who handle personal data will receive appropriate data protection training. This training will be refreshed periodically to

ensure ongoing awareness of responsibilities and changes in legislation or best practice.

13. Policy Review

This Data Protection Policy will be reviewed by Ynysybwl and Coed Y Cwm Community Council annually, or sooner if there are significant changes in legislation, guidance from the Information Commissioner's Office, or Council operations.

Last Reviewed: 29 May 2025
Next Review Due: May 2026

Appendix 1: How to Contact Us Regarding Data Protection

For any queries, requests, or concerns regarding data protection, please contact:

The Clerk to Ynysybwl and Coed Y Cwm Community Council

Email: clerk@ynysyblwcc.gov.uk
Telephone: 07951117876
Postal Address: The Old Police Station, Paget Street, Ynysybwl, RCT CF373LF

Complaints to the Information Commissioner's Office (ICO):

If you are dissatisfied with how we have handled your personal data, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

- **Website:** www.ico.org.uk
- **Telephone:** 0303 123 1113
- **Postal Address:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF