

**CLYDACH COMMUNITY COUNCIL**

**DATA PROTECTION POLICY**

**Introduction**

Clydach Community Council (the Council") is fully committed to compliance with the requirements of the **Data Protection Act 1998 (the Act")**, which came into force on the 1st March 2000 and the **General Data Protection Regulations (GDPR) (“the Regulations”)** which come into force on 25th May 2018.

The Council will therefore follow procedures that aim to ensure that all employees, elected members, members of the public, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under the Act and the Regulations.

**Statement of policy**

In order to operate efficiently, the Council has to collect and use information about people
with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act and Regulations to ensure this.

The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 and the General Data Protection Regulations.

**The principles of data protection**

The Act and Regulations stipulate that anyone processing personal data must comply with Principlesof good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for a specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection and the express permission of the data subject has been granted.
9. Everyone managing and handling personal information is appropriately supervised, has a legitimate reason and interest to do so, is trained and formally appointed to do so;
10. Any person or body wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows the process, including methods of contact.

The Act and Regulations provide conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

* That data;
* That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

* Racial or ethnic origin;
* Political opinion;
* Religious or other beliefs;
* Trade union membership;
* Physical or mental health condition;
* Sexual Orientation;
* Criminal proceedings or convictions.

Handling of personal/sensitive information

The Council will, through appropriate management and the use of strict criteria and controls:-

* Observe fully conditions regarding the fair collection and use of personal information;
* Meet its legal obligations to specify the purpose for which information is used;
* Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
* Ensure the quality of information used;
* Apply strict checks to determine the length of time information is held;
* Take appropriate technical and organisational security measures to safeguard personal information;
* Ensure that personal information is not transferred abroad without suitable safeguards;
* Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
* Will carry out Data Protection Impact Assessment (DPIA’s) for any activity, procedure or process where information is gathered, monitored or stored in any way.

These include:

* The right to be informed that processing is being undertaken;
* The right of access to one's personal information within 30 days;
* The right to prevent processing in certain circumstances;
* The right to correct, rectify, block or erase information regarded as wrong or irrelevant information.

In addition, the Council will ensure that:

* Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
* Everyone managing and handling personal information is appropriately trained to do so and has a legitimate reason.

All forms of data will only be stored in line with national guidelines, and will be disposed of by an approved date removal contractor. A receipt must be obtained and held on file by the council following removal of data from the premises.

* Queries about handling personal information are promptly and courteously dealt with;
* Methods of handling personal information are regularly assessed and evaluated;
* Performance with handling personal information is regularly assessed and evaluated; Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff within the Council's directorates will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

* Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
* Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically; Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the Council must:

* Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act and Regulations. Any breach of any provision of the Act or Regulations will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm; Allow data protection audits by the Council of data held on its behalf (if requested); Indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by the Council will be required to confirm that they will abide by the requirements of the Act and Regulations with regard to information supplied by the Council.

**Data Protection Officer**

a) The Council will ensure that it has a Data Protection Officer (DPO)

b) The DPO will monitor internal complains, informing and advising on the council’s data protection obligations. c) The DPO will advise regarding Data Protection Impact Assessments (DPIA’s) and act as a contact point for data subjects and the supervisory authority.

e) The DPO must be independent, an expert in data protection, adequately resourced and report to council chairperson on a regular basis.

f) The Community Council may choose to employ a DPO solely for its own purposes, or may share a single DPO with other organisations.

The Community Council have ultimate responsibility for the protection of data and must give due regard to advice provided by its Data Protection Officer.

The Community Council may gather and store information on individuals in its course of public duties as laid down in the Local Government Act 1974. Likely sources of data, their use and treatment are outlined below. These activities are also assessed using a Data Protection Impact Assessment (DPIA).

**Planning Applications**

In line with the Town and Country Planning Act 1990, planning applications are shared in the public domain. The Community Council will discuss planning applications, but will not discuss individual names or contact details (other than address) at any public meeting.

**Correspondence**

The Local Government Act 1974 required the Community Council to raise correspondence received at public meetings. A statement to this effect will be provided to those corresponding.

**Mailing Lists**

Where the council currently, or intends to develop a mailing list, those wishing to join must ‘opt in’ and will not be automatically enrolled onto a mailing list. The purpose of the mailing list must be clearly advertised. This list must not be used for any other reason, other than the reasons advertised. Those who opt in to any mailing list must be able to opt out of this list and any time and this must be clearly advertised to subscribers. The Community Council will not share this information with any other person or organization. Information must be minimal, in that it will collect a person’s email address, their name, age, address, telephone number and area of interest. No financial, medical or other personal information will be collected. In instances where the community council wishes to use a person’s information for reasons other than those reasons initially advertised, the council will contact the person in the first instance to obtain their express written permission.

**Funding Applications**

Where information regarding funding applications and projects is obtained, the council must obtain the data subject’s express written and signed permission to use any case study or photographs in any social media or marketing campaign. Where this is the case, the data subject will be provided with a full, detailed explanation of how their information will be used, and will be asked to ‘opt in’. No automatic assumption of opt in will be made.

**Social Media / Websites**

Social Media / Websites will not display any personal information relating to a data subject without their express permission. A declaration regarding the Data Protection Act and General Data Protection Regulations will be clearly displayed on the council’s website and social media site.

**CCTV**

The council has a legitimate interest in the provision of CCTV at its buildings to monitor employee contractual arrangements, health and safety and to monitor and minimize criminal activity. A CCTV Policy underlines in more detail requirements of the protection of data surrounding the council’s CCTV.

**Emails**

The council will naturally receive emails from organisations and individuals and will retain these to assist in responding on matters. Where the council emails a group of individuals or organisations, addressees will be BCC’d into emails so that each person does not see the other person’s email address.

1. n