Cyngor Cymuned Pontyclun Community Council

Council policy on Data Protection and Freedom of Information

last review May 2022

Contents

Manging our data and records

The Council stores considerable amounts of information within its files. This will be held

- Manually in our filing systems and long-term storage in the attic of Café 50.
- Electronically within our hard drives / cloud storage
- Electronically in our e-mail server.

Records should only be kept for as long as they are relevant to us or where we are required by statute to hold them.

Records will be filed away in relevant filing system and sensitive data will be protected by way of password (electronic data) and lock and key (manual data).

The Officers will make periodic reviews of our data and remove obsolete records in a secure way. RCT provide a service to destroy confidential data securely and the Council will use this when required.

Pending approval of specific guidelines tailored to this Council, to decide what is relevant and what can be destroyed the Council will follow the Guidelines published by One Voice Wale and the NALC. These consider statutory requirements and well as likely relevance e.g. tax law. Once the Council specific guidelines are drawn up and approved these will be used.

This document also outlines how we act in accordance with the key statutes relating to information. These include the General Data Protection Regulation (GDPR) Data Protection Bill (DPB) and the Freedom of Information act (FIA).

Information covered under this policy

The Acts are mainly concerned with "personal data", that is information about living, identifiable individuals. This need not be particularly sensitive information and can be as little as a name and address.

Individuals (data subjects) have certain rights. They require those who record and use personal information (data controllers) to be open about their use of that information and to follow sound and proper practices (the Data Protection Principles).

- **Data controllers** are those who control the purpose for which and the way personal data is processed.
- **Data Processors** are those who process the personal data
- **Data subjects** are the individuals to whom the personal data relate.

Data protection registration

The Council is registered by notifying the Information Commissioner's Office (ICO)

Data held at home by Councillors and staff

Staff and Councillors are not to hold personal data on behalf of the Council electronically on their computers other than on the Councils servers/e-mail system.

The exception to this is that publicly available contact information can be stored for ease of use. It is the responsibility of the person storing the data to ensure it is up to date and reviewed at least annually.

Where staff are using Council Computers/tablets/phones at home then they are covered by the Council's registration.

More guidance is provided for Councillors in a set of Guidelines issued by the Council.

Sensitive Data

The Act defines eight categories of sensitive personal data. These are:

(a) the racial or ethnic origin of data subjects;
(b) their political opinions;
(c) their religious beliefs or other beliefs of a similar nature;
(d) whether they are a member of a trade union:
(e) their physical or mental health or condition:
(f) their sexual life:
(g) the commission or alleged commission by them of any offence; or
(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The Council will only hold personal data falling into these categories once they have the consent of the individual concerned. Any such date will be held, and password protected (electronically) or locked away (manual data).

Manual Data

The acts also cover some records held in paper form. Such records need not be notified to the Commissioner, but we will handle them in accordance with the data protection principles.

Subject access requests

A subject access request gives individuals entitlement to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone to whom it may be disclosed, and any information available to you about the source of the data.

If we receive a written subject access request, we will deal with it promptly, and in any case within 40 days from the date of receipt.

If we need further information, the 40 days will begin when we receive this further information.

The Council does not charge a fee for these requests.

Freedom of Information requests

We are subject to the Freedom of Information Act 2000, which gives people the right to access information held by or on behalf of public authorities.

A person can make a request to the Council to have access to all recorded information held by it. This might be in the form of documents, emails, notes, audiotapes or letters and the information doesn't necessarily need to be about the person who requests the information from the Council.

A person can make a request to the Council in writing and in this request, the person must state their name and address and what information they want from the Council.

If the information which the person requests is already available in the Council's published documentation, then there is no need for the person to request this is writing as this can be downloaded from the Internet.

If a formal FOI request is made, then the Council has up to 20 days from the day after the date of the request to decide whether the law allows the requester to have the information.

If we can provide the information, then as much as possible should be provided. Should we be requested to provide information which will take longer than 18 hours to collect then we reserve the right to decline as it would cost too much to deal with the query. The Council will also charge to cover its costs in providing this data including –

- 5p per page for copies
- Postage costs
- Other direct costs incurred by the council
- Costs totalling less than £5 will not be billed

If the information which has been requested from the Council identifies other people, it cannot be disclosed and neither can information which may compromise national security.

Appendix 1 - The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of personal data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of personal data subjects in relation to the processing of personal data.

Appendix 2- Data Protection Officer

The GDPR introduces a duty for certain organisations to appoint a data protection officer (DPO), though Community Councils do not have to have one and we have chosen not to do so at this time.

- DPOs assist us to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases, several organisations can appoint a single DPO between them.
- DPOs can help us demonstrate compliance and are part of the enhanced focus on accountability.

DPO's are not personally responsible for non-compliance with the GDPR. The GDPR makes it clear that it is the controller or the processor who must demonstrate that processing is undertaken in compliance with the GDPR. Personal data protection compliance is the responsibility of the controller or processor.

Appendix 3 - Further Information

For Advice on Data Protection and Freedom of Information Issues:

Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF
Telephone: 0303 123 1113 or 01625 545 700

e-mail: mail@ico.gsi.gov.uk or notification@ico.gsi.gov.uk

Website: www.ico.gov.uk