



Fishguard & Goodwick Town Council

Cyngor Tref Abergwaun ac Wdig

Data Protection Policy

1. Introduction

The Town Council holds and processes information about employees, councillors, residents and customers, and other data subjects for administrative and commercial purposes.

When handling such information, the Town Council, and all staff or others who process or use the information, must comply with the Data Protection principles as set out in the General Data Protection Regulation (GDPR) 2018:

<https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

[General Data Protection Regulation \(GDPR\) 2018: Guidance for members](#)

2. Data Protection Principles

There are six general principles set out in the GDPR:

1. Personal information shall be processed fairly and lawfully and in a transparent manner.
2. Personal information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with the purpose
3. Personal information shall be adequate, relevant and limited to what is necessary.
4. Personal information shall be accurate and, where necessary, kept up-to-date.
5. Personal information shall only be retained only for as long as necessary.
6. Personal information shall be processed in an appropriate manner to maintain security.

You must have a lawful basis to process personal data. There are six available lawful bases, these are consent, contract, legal obligation, vital interests, public task, legitimate interests. No single basis is better or more important. Which is appropriate will depend on your purpose and the relationship with the individual.

3. Definitions

“Employees, councillors, residents and customers, and other data subjects” may include past, present and potential members of those groups.

“Other data subjects” and *“third parties”* may include contractors, suppliers, contacts, referees, friends or family members.

“Processing” refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

“Personal data” is information about an identifiable, living individual.

“Sensitive personal data” is personal data consisting of information relating to racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental health or condition, sexual orientation or criminal proceedings or convictions.

“Data Controller” is a ‘person’ who determines the purposes for which and the manner in which any personal data are, or are to be, processed. A ‘person’ as recognised in law may be an individual, organisation or body of persons.

“Data Protection Officer” is an individual working on behalf of the Data Controller with responsibility for the data protection within that organisation.

4. Responsibilities

Fishguard & Goodwick Town Council is the Data Controller and must ensure that any processing of personal data for which they are responsible complies with the Act.

The Data Protection Officer is the Town Clerk, who acts on behalf of the Council, and is responsible for:

- i. fully observing conditions regarding the fair collection and use of information.
- ii. meeting the Council’s legal obligations to specify the purposes for which information is used.
- iii. collecting and processing relevant information, only to the extent that is required to fulfil operational needs/to comply with legal requirements.
- iv. ensuring the quality of information used.
- v. applying strict checks to determine the length of time that information is held.
- vi. ensuring that the rights of the people whom information is held are able to be fully exercised under the Act.
- vii. taking appropriate technical and organisational security measures to safeguard personal information.
- viii. ensuring that personal information is not transferred abroad without suitable safeguards.
- ix. ensuring that everyone managing and handling personal information:
 - a. fully understands that they are contractually responsible for following good practice in terms of protection.
 - b. is adequately trained to do so.
 - c. are appropriately supervised.

5. Storage and Retention

Personal data is kept in paper-based systems and/or on a password-protected computer system.

The Council will keep different types of information for differing lengths of time, depending on legal and operational requirements. Please ask the Clerk if you require any further information on this.

6. Access to Information

Any employees, councillors, residents, customers and other data subjects have a right to:

- i. ask what personal information the Council holds.
- ii. ask what this information is used for.
- iii. be provided with a copy of the information.
- iv. be given details of the purposes for which the Council uses the information and any other persons organisations to whom it is disclosed.

- v. ask that any incorrect data held is corrected.

The Council's Data Protection Request Procedure sets out the process to be followed for data subjects wishing to make Subject Access Requests.

If it is felt by the data subject that any personal information held is incorrect the individual may request that it be amended. The Council must advise the individual within 21 days whether or not the amendment has been made.

7. Breach of Policy

Compliance with the Act is the responsibility of all councillors, residents, customers and members of staff. Any deliberate or reckless breach of the policy may lead to disciplinary action and where appropriate, legal proceedings.

Any individual who believes that the Council has breached any of the requirements of the General Data Protection Regulation (GDPR) 2018 should raise the matter with the Data Controller initially either with councillors or the Town Clerk. Alternatively, a complaint can be made to the Information Commissioner:

<https://ico.org.uk/for-organisations/advice-for-small-organisations/contact-us-sme/>

Guidelines for Staff Members, Volunteers and Councillors

During the course of your duties with Fishguard & Goodwick Town Council, you will be dealing with information such as names/addresses/phone numbers/email addresses of members of the public. You may be told or overhear sensitive information while working for the Town Council.

General Data Protection Regulation (GDPR) 2018 gives specific guidance on how this information should be dealt with by organisations such as Fishguard & Goodwick Town Council. In short, to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To help you meet the terms of the Data Protection Act while working for Fishguard & Goodwick Town Council, the following guidelines have been drawn up. Please read them carefully and ask the Data Protection Officer (Town Clerk) if you are in any doubt about any of them.

Sharing members'/clients' personal information

"Personal information" includes details such as names/addresses/phone numbers/email addresses and health details supplied by members of the public.

Such information may be shared between staff and Councillors at Fishguard & Goodwick Town Council for work reasons but should not be given to anyone outside the Council without explicit consent from the member/client.

If such a situation arises, please ask the Town Clerk for advice.

Unlawful disclosure of personal information

Under the Data Protection Act you are committing a criminal offence if you disclose personal information 'knowingly or recklessly' to anyone you are not supposed to, so please be careful.

Give consideration to any conversations you are having containing personal or sensitive information that could possibly be overheard by people who should not have access to such information.

Use of files, books and other paper records

In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, please take good care of the files, books and other paper records you use while on duty and ensure that they are stored safely before you leave the building.

Use of email

Be sure before sending emails that it contains no personal or sensitive information that the recipients should not have access to. This is a particular risk when forwarding emails or adding in new recipients to an email chain.

Disposal of scrap paper

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Such notes must be shredded, there is a shredder in the Clerk's office that you are able to use.

Policy Reviewed: December 2023

Date Policy adopted: 5th December 2023