DATA PROTECTION POLICY

Reviewed and adopted on 18th July 2023

1. The General Data Protection Regulation 2018
The General Data Protection Regulation (GDPR) came into effect in the UK on 25 May 2018. It replaced the existing law on data protection (Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by councils. Odiham Parish Council must comply with its requirements.

2. The purposes of the GDPR are:

- To increase the obligations on organisations when acting as data controllers and processors.
- To increase the rights of individuals to ensure that their personal data is respected and only used for legitimate purposes.

3. Definitions:
Personal Data – is any information about a living individual which allows them to be identified from that data such as name, address, email address, photograph etc.
Data Controller – is the person or organisation who determines how and what data is processed.
Data Processor – is the person(s) or firm that process the data on behalf of the data controller.
Data Subject – is the individual about whom the personal data is processed.
Data Protection Officer – is the individual with responsibility for ensuring data protection compliance.
Consent – is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be given freely, provided on an opt-in basis rather than opt-out.

4. The Parish Council's Commitment
As a local authority and a data controller, Odiham Parish Council will comply with the underlying principles that personal data:-

(a) Must be processed lawfully, fairly and transparently.
(b) Is only used for ***specific legitimate processing purposes*** and not further processed in a manner incompatible with those purposes;
(c) Should be ***adequate, relevant and limited*** i.e. only the minimum amount of data should be kept for specific processing.
(d) Must be ***accurate*** and where necessary ***kept up to date***.
(e) Should ***not be stored for longer than is necessary***, and that storage should be safe and secure.
(f) Should be processed in a manner that ensures ***appropriate security and protection.***

5. Personal Data Processed
The personal data kept or processed by OPC includes but is not confined to the following:

- Names, titles and aliases, photographs and video images;
- Contact details such as telephone numbers, addresses and email addresses, social media addresses;
- Financial identifiers such as bank account numbers, payment card details for staff, contractors and for suppliers;
- Demographic and background information on staff and members including gender, age, marital status, employment background and qualifications;
- Some sensitive personal data in relation to staff and members such as racial/ethnic origin, mental and physical health and trade union affiliation;
- Website data such as IP address and analytical data;

6. How/Why Personal Data is used
- To deliver public services;
- To confirm identity to provide some services;
- To enable the council to meet its legal and statutory obligations and powers including delegated functions;
- To contact individuals and organisations;
- To maintain accounts and records;
- To process financial transactions;
- To protect public funds and facilities;
- To recruit and employ staff and contractors;

7. Lawful Bases for Processing Personal Data

The Council is a public authority and has certain powers and obligations. Most personal data is processed for compliance within its public task which includes the discharge of the council's statutory functions and powers.

There are six lawful bases for processing data under the GDPR:

1. **Consent**
   The controller must be able to demonstrate that consent was given. Consent to process data will be sought from individuals whenever public consultations are carried out.
2. **Legitimate interests**
   This involves a balancing test between the controller and the interests of the fundamental rights and freedoms of the data subject. Councils cannot rely on legitimate interests as a legal basis for processing personal data.
3. **Contractual necessity**
   Personal data may be processed if necessary in order to enter into or perform a contract with the data subject.
4. **Compliance with legal obligation**
   Personal data may be processed if the controller is legally required to perform such processing.
5. **Vital interests**
   Personal data may be processed to protect the vital interests of the data subject.
6. **Public task**
   Personal data may be processed if the processing is necessary for the performance of tasks carried out by the Council in compliance with its legal obligations, statutory powers and functions. As a local authority, much of Odiham Parish Council's processing will fall under this lawful basis. This lawful base will be used to process personal data when residents write to councillors or office staff. This data will not be shared outside the Council without the consent of the individual.

8. Individual's Rights

Individuals have:

- The right to be informed – via privacy notices and an explanation of the lawful basis for the processing.
- The right to access the personal data the council holds on that individual – via a subject access request;
- The right to correct and update their personal data;
- The right to have their personal data erased (The right to be forgotten);
- The right to restrict processing;
- The right to data portability;
- The right to object to processing;
- The right not to be subject to automated decision-making including profiling.

9. Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a type of audit used to help assess privacy risk. OPC will evaluate if a DPIA is required when considering new processing operations. DPIA are mandatory where processing poses a high risk to the rights and freedoms of individuals.

10. Data Protection Compliance Officer

OPC has appointed the Parish Clerk as the Data Protection Compliance Officer. Their duties include:

- Informing the council and its staff of their obligations on GDPR and other data protection legislation;
- Monitoring compliance of the council, both in its policies and practices; Raising awareness of data protection law; providing training and advice; Carrying out data protection-related audits;
- Acting as a contact point for the Information Commissioner's Office.

11. Related Policies and Notices

These include:

- Document Retention Policy
- Subject Access Request Policy
- Privacy Notices

12. Information Commissioner's Office

In the UK the Information Commissioner's Office are responsible for upholding information rights in the public interest. They are responsible for investigating data misuse and have the authority to impose penalties.