

# ASHFORD HILL with HEADLEY PARISH COUNCIL

## Data Protection Policy

### Introduction

The Parish Council hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes. This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires Officers to ensure that the Data Protection Officer (DPO) i.e. the Clerk to the Council, be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

### Business purposes

The purposes for which personal data may be used by the Parish Council:

- Personnel,
- Administrative,
- Financial,
- Statutory and legislative purposes,
- Payroll,
- Consultations and business development purposes.

Council purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring Council policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions
- Training and quality control
- Ensuring the confidentiality of sensitive information
- Security vetting and checking
- Investigating complaints
- Checking references
- Ensuring safe working practices, administration and assessments

## **Our procedures**

### **Fair and lawful processing**

The Parish Council must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the Council updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Assisting with data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, council members and other stakeholders
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by Chinnor Parish Council
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing

Responsibilities of the Officers

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice relating to on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers, employees, residents and service users
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that service users and correspondents have a right of access to the personal data that we hold about them

## **Sensitive personal data**

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

## **Accuracy and relevance**

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

## **Your personal data**

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the DPO so that they can update your records.

## **Data security**

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

## **Storing data securely**

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data

- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the council's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall

## **Data Retention**

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

## **Subject Access Requests**

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. If you receive a subject access request, you should refer that request immediately to the DPO. Who may ask you to help us comply with those requests. Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law. Processing data in accordance with the individual's rights You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request. Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed. Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

## **Training**

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure. Training is provided through an in-house seminar on a regular basis. It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures. Completion of training is compulsory.

**Adopted July 2024**