Personal Data Protection Policy

Purpose of this policy

This policy statement explains Farnsfield Parish Council's responsibilities regarding the protection of personal data. Staff and members should read, understand and apply this policy and any other documents referenced in it and refer any concerns to the Clerk or to Council.

Personal data is any information about a living individual from which they can be identified, such as a name, video, email, or address. Identification can be directly using the data itself or by combining it with other information.

Our privacy notice explains what personal data we hold, the reason for holding it, where it came from, when it will be deleted and also the rights and responsibilities of individuals. The privacy notice is available on our website or from the Clerk at clerk@farnsfield-pc.uk along with all policies and procedures referenced in this document. This policy will be reviewed annually or when needed.

What is Data Protection?

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses and government and is the UK's implementation of the General Data Protection Regulation (GDPR). Farnsfield Parish Council is registered with the Information Commissioner's Office (ICO) as a data controller for the purposes of processing personal data and is committed to complying with the data protection law.

Responsibilities of Staff and Council Members for Data Protection

In order to comply with the Data Protection Act, staff and members of Farnsfield Parish Council must ensure the following.

- Personal data should be kept confidential, for example, Blind Copy (BCC) should be used to avoid sharing email addresses when appropriate, such as for working group members.
- Correspondence, complaints or queries should remain confidential and only shared for legitimate reasons.
- Personal data should only be collected where the purpose is detailed in our **Privacy Notice.**
- Personal data should only be processed for the purpose detailed in our **Privacy Notice.**
- Personal data should be accurate and if not, it should be corrected.
- Personal data no longer needed should be deleted, shredded or securely disposed of in line with our records retention schedule available in our **Records Management and Security Policy**.
- Personal data should be kept securely and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage or unauthorised disclosure. Hardcopy personal data is stored securely in the Council office. Care should be taken to ensure that personal data is kept confidential and secure if photocopied, printed or saved onto cloud storage or removable media such as a usb stick or onto a personal device such as a laptop, phone or iPad. Devices should be password protected and protected from spyware, viruses and malware. Where appropriate files should be password protected.

This list is not conclusive. Staff and members are expected to "think privacy" and to consider the impact of any actions in relation to personal data carefully and if in doubt to ask for advice.

Subject Access Requests

Individuals have the right to access any personal information that is held about them. Subject Access Requests must be submitted in writing by letter or email. The response will be within 30 days and is free of charge. Our **Subject Access Requests Procedure** is available on our website or from the Clerk