FITZHEAD PARISH COUNCIL DATA PROTECTION POLICY 2026

This policy was adopted by the Council on 13 August 2026

1. Introduction

Fitzhead Parish Council ('the Council') has responsibilities under the Data Protection Act 2018(DPA 2018), UK General Data Protection Regulation (UK GDPR), Data (Use and Access) Act 2025 (DUAA), Local Government Acts and the Human Rights Act 1998 to protect rights of privacy and ensure that personal data is sufficiently protected when it is being processed.

The Council is required as part of its overall information governance structure to ensure that appropriate controls are implemented and maintained in the collection and use of personal information and that these are in accordance with the requirements of the current data protection law (the DPA 2018 and the UK GDPR along with other legislation).

In most cases the Council will be the data controller for the personal data it processes. A data controller is the organisation or person who determines and controls the purpose for the processing of personal data.

There may also be circumstances in which the Council has appointed a third party to process data on its behalf and in such circumstances that party will be a data processor, but the Council will remain the data controller.

This policy sets out the Council's approach to complying with the above legislation in relation to data protection.

2. Scope

This policy applies to applies to all employees, councillors, contractors, volunteers or any other persons who have access to, or use the Council's information.

Personal data is defined as: Any information related to an identified or identifiable living natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identifications number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category personal data is defined as personal data relating to any of the following

- Racial or ethnic origin.
- Political opinions.
- Religious or Philosophical beliefs.
- Trade Union membership.
- Genetic or biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Sex life or sexual orientation.

3. Principles of Good Practice

The UK GDPR includes seven key principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

All employees processing personal data must ensure they adhere to the principles as defined in the data protection law which require that personal data is:

- Used fairly lawfully and transparently.
- Used for specified, explicit and legitimate purposes.
- Used in a way that is adequate, relevant and limited to only what is necessary.
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary for the purposes for which it was collected.
- Handled in a way that ensures appropriate security including protection against unlawful or unauthorised processing, access, loss destruction or damage.
- Accountability- As a data controller the Council is responsible for complying with the above principles and must be able to demonstrate compliance.

4. Access and use of Personal Data

This policy applies to everyone that has access to personal data and includes any third party who conducts work or voluntary activity on behalf of the Council or who has access to personal data for which the council is responsible.

It is an offence for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller.

All data subjects are entitled to:

- Be informed about how data is being used.
- Access personal data.
- Have incorrect data updated.
- Have data erased.
- Stop or restrict the processing of data.
- Data portability (allow data subjects to get and reuse data for different services).
- Object to how data is being processed in certain circumstances.
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects.

The above rights are not absolute and only apply in certain circumstances

The Council will process all personal data in accordance with the relevant legislation. Where the Council is seeking to pursue a new project that involves the use of personal data, a data protection impact assessment will be carried out to assist the Council in systematically analysing, identifying and minimising the data protection risks.

The Council will only process personal data where it complies with the data protection principles under the legislation and in doing so will only process the minimum personal data required for the intended purpose. The Council will also seek to use anonymised data where

appropriate to do so to avoid the retention of personal data where it is not necessary to retain it.

In the collection and retention of personal data, the Council will take reasonable steps to ensure that the personal data held is accurate, up-to-date and not misleading.

All personal data will be retained in accordance with the Council's retention schedule.

The Council holds a data map, which includes information about data processing activities and any systems that process personal information.

Personal data will be processed and stored by the Council in accordance with the Council's IT Policy.

Where the Council appoints a third party to process personal data on its behalf, it will enter into a data processing agreement with the third party to ensure that the personal data is sufficiently protected. The Council will ensure that information processed by third parties is done so in line with legal requirements and good practice. The Council has privacy notices which explain why it collects personal data, how that personal data is used and shared (if applicable), and the rights that people have over their personal data.

5. Sharing Personal Data

There may be a need for the Council to share personal data that it holds with another party, in which case it will only do so where it has a legal obligation, power or permission to do so. Where appropriate, individuals will be informed that their personal data is being shared and any personal data shared will be undertaken confidentially and securely.

The Council will ensure that data sharing agreements are in place (where appropriate) to set out the terms on which personal data will be shared with another party.

Where personal data is being transferred, the Council will endeavour not to transfer personal data outside of the European Union, to third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by data protection legislation.

Personal data within the Council will only be accessed by those employees and Members that need to access the information for their role and business need.

6. Data breaches

Where there has been a breach of data protection legislation, the Council will consider whether it is appropriate and necessary to report the breach to the Information Commissioner's Office.