

# KIRKBY FLEETHAM WITH FENCOTES PARISH COUNCIL

## DATA PROTECTION POLICY

### Introduction

1. Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.
2. It sits alongside and supplements the UK GDPR (General Data Protection Regulation) - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.
3. The main elements of the Act are:
  - a. Implements GDPR standards across all general data processing and provides clarity on the definitions used in the GDPR in the UK context.
  - b. Empowers people to take control over their data.
  - c. Provides appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification,
  - d. Enacts additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
  - e. Allows the Information Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches.

### Data Processing Principles

4. Those that determine how and why personal data is processed must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection legislation.
5. Members processing personal data must comply with the six enforceable principles of good practice. Personal data must be:
  - a. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
  - b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
  - c. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
  - d. Accurate and, where necessary, kept up to date.
  - e. Kept in a form that permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed.
  - f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. The council will tell you of the personal data it processes, the reasons for processing your personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

7. The council will not use personal data for an unrelated purpose without telling the individual about it and the legal basis that we intend to rely on for processing it. The council will not process personal data if it does not have a legal basis for processing.

### **Duties and Responsibilities Under the Act**

8. Kirkby Fleetham with Fencotes Parish Council is committed to complying with the principles of the Data Protection Act. It will follow procedures designed to provide that all elected members, employees, contractors, consultants, partners, or other servants or agents of the Parish Council (collectively referred to as "the data users") who have access to any personal data held by or on behalf of the Parish Council are fully aware of and abide by their duties and responsibilities under the Act.

9. The Parish Council has nominated the Parish Clerk to be responsible for co-ordinating all data protection issues, for the receipt of subject access requests and the co-ordination of and compliance with the requirements of the Act when such requests are received.

10. Personal data is to be relevant, adequate and not excessive for those processing purposes it is intended.

11. All personal data will be processed fairly and lawfully. In particular, form and document design will be kept under review, to ensure compliance with the data protection principles under the Act.

12. All processing of personal data by the Parish Council will be subjected to a risk assessment, taking into account:

- a. The likelihood of a breach of the data protection systems.
- b. The potential impact on the data subject, elected members, managers or staff.
- c. The level of controls in place with regard to the data together with the setting and testing of clear controls to minimise breaches of the Act.

13. No disclosure of data is to be undertaken by any data user which breaches any of the provisions of the Act, as interpreted by the Parish Council, the Commissioner or the courts.

14. All elected members of the Parish Council are to be data users and as such will not be required to register as data processors in their own right, but will be part of the Councils registration.

15. All data users are to be made aware of this policy and their duties and responsibilities under the Act.

16. The Parish Council regards any unlawful breach of any provision of the Act by any employee as being a disciplinary matter. Any employee(s) who breach this policy will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct.

17. The Council will maintain a Data Protection Policy which will be available on the Parish Council website.

18. The Parish Council will undertake an annual review of all data protection systems and controls to ensure compliance with the Act, this policy and codes of practice, including data security.

19. All contractors, consultants, partner or other servants or agents of the Parish Council must:

a. Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Parish Council are aware of this policy and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Parish Council and that individual, company, partner or firm.

b. Promptly, pass any subject access requests relating to the Council's business to the Clerk and provide that person with any information needed by them to comply with the subject access request.

c. Indemnify the Parish Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

20. All data users will ensure that appropriate security measures are undertaken to safeguard personal data, commensurate with the nature of the data concerned.

### **Subject Access Requests**

21. Subject Access Requests (SAR) must:

a. be made in writing or by email to the Parish Clerk.

b. include full name, address and contact telephone number.

c. include any information to identify or distinguish from someone of the same name.

d. include details of the specific information required and any relevant dates.

22. The Parish Council will respond to the request promptly, within one calendar month. 'Day one' is the **day of receipt** – for example, a SAR received on 3 September should now be responded to by 3 October. The time limit is calculated from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. If further information is required, day one will commence from the date that further information is obtained.

23. Under the Act, provision is made for the Parish Council to ask for an administration fee of not more than £10.00 and the time frame does not begin until that fee has been paid.

24. Information will be provided to the applicant in the format requested and may be in the form of copy or summary, or the applicant may request to inspect the record. Exemptions under the Act will be enforced.

25. In response to a SAR, individuals are entitled to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone it may be disclosed to, and any information available about the source of the data.

26. If a SAR is manifestly unfounded or excessive, the council is not obliged to comply with it. A SAR is likely to be manifestly unfounded or excessive where it repeats a request to which

the council has already responded. If you submit a request that is unfounded or excessive, the council will notify you that this is the case and whether or not we will respond to it.

27. The Parish Clerk is to maintain a register indicating the information that has been provided in response to SARs.

**Data Breaches**

28. The council have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the council must take notes and keep evidence of that breach.

29. If you are aware of a data breach you must contact the Clerk or Chairman of the Parish Council immediately and keep any evidence, you have in relation to the breach.

30. If the council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner and data subjects within 72 hours of discovery. The council will record all data breaches regardless of their effect.

|                   |  |
|-------------------|--|
| Version:          | 1.0  |
| Adoption Date:    | September 2023   |
| Author:           | Councillor Jones   |
| Reference:        | Data Protection Act 2018   Revised 2021<br>NALC, Legal Topic Note 38 – Data Protection |
| Reviewed By:      | Full Council   |
| Next Review Date: | September 2024   |