Feckenham Parish Council Data Protection Policy

1. Introduction

Feckenham Parish Council (FPC) is committed to protecting personal data in compliance with the **Data Protection Act 2018**, the **UK General Data Protection Regulation (UK GDPR)**, and other applicable information compliance legislation. This policy outlines our obligations, responsibilities, and procedures for managing personal data securely, lawfully, and transparently. From the 2025/26 financial year, as required by the Annual Governance and Accountability Return (AGAR), we must confirm robust compliance with digital and data protection standards—including enhanced oversight of our digital systems—as specified in Assertion 10.

2. Compliance with AGAR Assertion 10

In recognition of increased scrutiny of digital and data protection practices under AGAR Assertion 10, FPC commits to:

- Explicitly designating leadership responsibilities for both traditional and digital data compliance.
- Conducting regular cybersecurity audits and risk assessments.
- Implementing advanced security measures (such as encryption, multi-factor authentication, and access controls) for digital records.
- Ensuring up-to-date training for staff and councillors on digital risks and data protection practices.
- Demonstrating our compliance through annual reviews and documentation in our AGAR submissions.

3. Scope

This policy applies to all personal data processed by Feckenham Parish Council, regardless of its form—whether electronic or paper. It covers data collected and processed in relation to:

- Councillors, employees, contractors, and volunteers;
- Residents, customers, and other data subjects, including past, present, and potential members of these groups.

4. Key Data Protection Principles

FPC adheres to the following principles as mandated by the UK GDPR and supporting legislation:

1. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed in a fair, lawful, and transparent manner.
2. **Purpose Limitation:** Data will be collected solely for specified, explicit, and legitimate purposes and will not be further processed in any incompatible manner.
3. **Data Minimisation:** Only data that is adequate, relevant, and limited to what is necessary for the intended purpose will be collected.
4. **Accuracy:** Personal data must be accurate and, where necessary, kept up to date.
5. **Storage Limitation:** Data shall not be stored longer than is necessary for the purposes for which it is processed.
6. **Integrity and Confidentiality:** Appropriate technical and organisational measures shall be implemented to ensure data security against unauthorised processing, accidental loss, damage, or destruction.
7. **Accountability:** FPC will take responsibility for ensuring and demonstrating compliance with these data protection principles.
8. Not be transferred to a country outside the European Economic Area, unless that country has the equivalent levels of protection for personal data, except in specified circumstances.

5. Roles and Responsibilities

Data Controller and Overall Accountability

Feckenham Parish Council is the designated Data Controller and is responsible for ensuring that every aspect of personal data processing complies with legal standards.

Digital Compliance and Leadership

While parish councils are not legally mandated to appoint a full-time Data Protection Officer (DPO), FPC designates the Clerk as the Lead on Compliance. Responsibilities include:

- Monitoring both traditional and digital data processing to ensure full compliance with the Data Protection Act 2018 and UK GDPR.
- Overseeing digital security measures, including cybersecurity audits and the implementation of access controls.
- Providing advice, support, and training to councillors, employees, contractors, and volunteers on all data protection matters.
- Acting as the primary point of contact for any data protection queries or breaches.

6. Storage, Retention, and Digital Security

Storage and Physical Security

- Paper Records: Personal data stored on paper must be kept in secured, locked locations when not in use.
- Digital Records**:** Personal data stored on computer systems must be protected by password controls, restricted access, and regular backups.

Retention

- Data will be retained only for as long as necessary to fulfil legal, operational, or reporting purposes.
- Different types of data are subject to different retention periods according to statutory and regulatory requirements.

Digital Security Measures

To address modern digital challenges, FPC implements:

- **Encryption:** Personal data stored digitally is encrypted to prevent unauthorised access.
- **Multi-Factor Authentication:** Access to digital systems requires multi-factor authentication.
- **Regular Cybersecurity Audits:** Scheduled risk assessments and security evaluations ensure that vulnerabilities are identified and mitigated.
- **Ongoing Staff Training:** Regular digital security training sessions keep all relevant personnel up-to-date on best practices and emerging threats.

7. Rights of Data Subjects

Data subjects have the following rights:

- **Access:** Request details of the personal data held by the council.
- **Purpose:** Understand and receive clarification about how the data is used.
- **Correction:** Request correction of inaccurate or incomplete data.
- **Deletion:** Seek deletion of personal data where applicable.
- **Transparency:** Receive details of any third parties with whom the personal data is shared.

Requests to access or correct data will be addressed promptly, with data subjects typically informed of outcomes within 21 days.

8. Reporting, Incident Response, and Breach Management

General Breach Response

- Any breach—deliberate or accidental—must be reported immediately.
- The appointed Lead on Compliance (Clerk) will initiate an internal investigation and, where necessary, notify the appropriate authorities.

Digital Breach Protocol

- In the event of a digital data breach, an incident response plan will be activated. This plan includes:
  - Immediate containment procedures.
  - Communication protocols both internally and externally.
  - Post-breach analysis to identify the cause and prevent recurrence.
- Detailed records of all breaches will be maintained and used for continuous improvement of our digital security posture.

9. Guidelines for Staff, Volunteers, and Councillors

Sharing of Personal Information

- **Internal Sharing:** Personal data sharing is permitted among council staff and councillors solely for the purposes of fulfilling council duties.
- **External Sharing:** No personal data should be communicated to external parties without the explicit consent of the individual concerned or unless required by law.
- **Sensitive Information:** Exercise extra caution when handling sensitive data (e.g., health details or personal opinions).

Email and Digital Communications

- Ensure emails and other forms of digital communication do not contain personal or sensitive data unless using secure, approved methods.
- Avoid forwarding emails or adding new recipients without ensuring that all parties are authorised to view the included data.

Handling of Physical Documents

- Maintain proper storage of physical records in secure areas to prevent unauthorised access.
- Lock away files and documents when not in use and during non-operational hours.

Training and Awareness

- All persons with access to personal data are required to take part in training sessions on data protection and digital security.
- Regular briefings will be provided to ensure that everyone understands their responsibilities and remains updated on legislative and procedural changes.

10. Policy Review and Updates

Feckenham Parish Council will review this Data Protection Policy at least annually—or whenever significant changes to the legal framework or our data processing practices occur. Updates will be incorporated promptly, ensuring ongoing alignment with both traditional data protection measures and modern digital compliance requirements, especially for future AGAR submissions.

This merged document ensures that all facets of data protection—from physical security and data retention to digital compliance and cybersecurity—are comprehensively addressed. It not only meets but strengthens our commitment to upholding high standards as outlined under the Data Protection Act 2018, UK GDPR, and AGAR Assertion 10.