Feckenham Smaller Authority Data Protection Policy

For Feckenham Parish Council

1. Introduction

Feckenham Parish Council, operating as a smaller authority for AGAR and proper practices purposes, 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 FPC's 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), FPC must confirm robust compliance with digital and data protection standards, including enhanced oversight of 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:

- Maintaining clear leadership responsibility for data protection and digital compliance, proportionate to FPC's size and staffing arrangements.
- Using the Data Roadmap to record and review data mapping, lawful bases, risks, compliance actions and evidence supporting AGAR Assertion 10.
- Applying the IT Policy to set expectations for secure and lawful use of IT equipment, software, email, online accounts and personal devices used for council business.
- Implementing proportionate technical and organisational safeguards for digital records, including access controls, strong passwords, secure backups and additional controls such as multi-factor authentication or encryption where appropriate and available.
- Providing appropriate awareness and guidance to councillors and volunteers, recognising that the Clerk is FPC's only employee.
- Demonstrating compliance through policy reviews, documented decisions, the Data Roadmap and supporting records for AGAR purposes.

3. Scope

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

- Councillors, employees, contractors, and volunteers;
- Residents, service users, correspondents, complainants, applicants 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. **Accountability evidence:** FPC will maintain appropriate policies, records and review arrangements to demonstrate compliance with data protection requirements.

International Transfers

Personal data shall not be transferred outside the United Kingdom unless the transfer is permitted under UK GDPR and appropriate safeguards, adequacy arrangements or legal exemptions are in place.

5. Roles and Responsibilities

Data Controller and Overall Accountability

FPC is the designated Data Controller and is responsible for ensuring that personal data processing complies with legal standards.

Digital Compliance and Leadership

As FPC's only employee, the Clerk is designated as the Lead Officer for data protection and digital compliance and acts as the main point of contact for data protection matters. The Clerk is not designated as a Data Protection Officer unless FPC formally resolves otherwise.

- Co-ordinating day-to-day compliance with the Data Protection Act 2018, UK GDPR and related council policies.
- Maintaining and reviewing the Data Roadmap as the working record of data mapping, lawful bases, compliance actions, risks and AGAR evidence.
- Applying the IT Policy to council business, including use of council systems, approved email arrangements, passwords, access controls, secure storage, personal devices and incident reporting.
- Ensuring retention and disposal decisions are made in accordance with the approved Retention Policy and any supporting retention schedule.
- Providing practical advice and reminders to councillors, contractors and volunteers on data protection and secure handling of council information.
- Acting as the primary point of contact for data protection queries, subject access requests and suspected personal data 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

- Personal data will be retained only for as long as necessary to fulfil legal, operational, financial, audit or reporting purposes.
- Retention periods, disposal arrangements and records management requirements are set out in FPC's approved Retention Policy and any supporting retention schedule.
- The Data Roadmap may be used to record relevant data holdings, retention considerations and actions required to improve compliance.

Digital Security Measures

FPC will take a proportionate, risk-based approach to digital security, reflecting its size, functions, staffing and the sensitivity of the personal data it holds. Detailed expectations for secure and lawful use of IT are set out in the IT Policy, with supporting

actions and evidence recorded through the Data Roadmap where appropriate. Measures may include:

- **Access controls:** limiting access to personal data to those who need it for council business and reviewing access when roles change.
- **Passwords and account security:** using strong passwords, keeping credentials confidential and applying multi-factor authentication where appropriate and available.
- **Secure storage and transmission:** using approved systems and reasonable safeguards for electronic records, including encryption where appropriate to the risk and system capability.
- **Backups and continuity:** maintaining suitable backup or recovery arrangements for important council records, proportionate to FPC's operating arrangements.
- **Review and improvement:** reviewing risks, incidents and practical improvements through the IT Policy, Data Roadmap and annual governance processes.
- **Awareness and training:** making GDPR and data protection training or briefing materials available to councillors, volunteers and the Clerk, recognising that councillors share responsibility for protecting council information and that the Clerk is FPC's only employee.

Relationship with Other Policies

This policy should be read alongside FPC's IT Policy, Retention Policy, Data Roadmap, privacy notices and any related procedures for subject access requests, Freedom of Information requests, publication, accessibility and incident reporting. These documents work together so that operational detail is maintained in the most appropriate policy or record, while this policy sets out the overall data protection framework.

7. Rights of Data Subjects

Individuals have rights under UK GDPR in relation to their personal data. These rights are not absolute and may be subject to legal conditions, exemptions or the lawful basis relied upon by FPC. Where a right does not apply, FPC will explain this in its response.

- **Right to be informed:** to receive clear information about how and why personal data is collected, used, shared, retained and protected.
- **Right of access:** to request confirmation that personal data is being processed and to receive a copy of that personal data and relevant supplementary information.
- **Right to rectification:** to request correction of inaccurate personal data or completion of incomplete personal data.
- **Right to erasure:** to request deletion of personal data where the right applies, subject to any legal, audit, public task or records retention requirements.

- **Right to restrict processing:** to request that FPC limits the way personal data is used in certain circumstances.
- **Right to data portability:** to receive personal data in a structured, commonly used and machine-readable format where this right applies.
- **Right to object:** to object to processing in certain circumstances, including processing based on public task or legitimate interests where applicable.
- **Rights relating to automated decision-making and profiling:** to be protected from certain decisions made solely by automated means. FPC does not normally undertake automated decision-making or profiling.

Requests relating to data subject rights will be acknowledged and handled without undue delay and within the statutory timescales required by UK GDPR and the Data Protection Act 2018. Where the law permits an extension, the data subject will be informed of the reason for the extension and the expected timescale.

8. Reporting, Incident Response, and Breach Management

General Breach Response

- Any actual or suspected personal data breach, whether deliberate or accidental, must be reported to the Clerk as soon as it is identified.
- As Lead Officer for data protection and digital compliance, the Clerk will co-ordinate the initial response, including containment, investigation, risk assessment and any immediate corrective action required.
- FPC will assess each breach promptly to determine whether it is likely to result in a risk to the rights and freedoms of individuals and whether notification to the Information Commissioner's Office or affected individuals is required by law.
- Where notification is required, FPC will act within the statutory timescales and maintain a record of the decision-making process.

Digital Breach Protocol

- Where a breach involves digital systems, devices, email, online accounts or electronic records, FPC will follow the relevant incident reporting and security requirements in the IT Policy and record any actions through the Data Roadmap where appropriate.
- The response may include immediate containment, securing accounts or devices, preserving evidence, reviewing access permissions, communicating with affected parties where appropriate, and taking proportionate steps to reduce the risk of recurrence.

- All personal data breaches, including those not reported externally, will be documented with the facts of the incident, effects, remedial action, notification decisions and any follow-up improvements.

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:** Personal data should only be shared externally where there is a lawful basis for doing so, where sharing is necessary and proportionate, and where appropriate safeguards are in place.
- **Special Category Data and Other Sensitive Information:** Special category data and other sensitive information, such as health information or information requiring particular confidentiality, must be handled with extra care and only where a lawful basis and any required additional condition apply.

Email and Digital Communications

- Personal data should only be included in emails or other digital communications where necessary for council business, and appropriate care should be taken to ensure it is sent securely and only to authorised recipients.
- Avoid forwarding emails or adding new recipients without ensuring that all parties are authorised to view the included data.
- Councillors use their own devices for council business and are expected to comply with the IT Policy when accessing, storing, sending or deleting council information on those devices.

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

- GDPR, data protection and digital security training or briefing materials will be made available to councillors, the Clerk and, where relevant, volunteers or contractors who handle council information. Many councillors may already be familiar with similar requirements through current or previous roles; the IT Policy provides a useful reference point for further data protection training and guidance where required.

- Councillors are encouraged to remain mindful of their data protection responsibilities, particularly when handling personal data or council information on their own devices for council business.
- The Clerk, as Lead Officer and FPC's only employee, will support awareness by signposting the relevant training and guidance identified in the IT Policy, sharing reminders where appropriate, and maintaining proportionate records of training, briefings or guidance provided.
- Regular updates or reminders will be provided where there are relevant legislative, procedural, IT security or policy changes.

10. Policy Review and Updates

FPC will review this Data Protection Policy at least annually, or whenever significant changes to the legal framework, AGAR requirements, proper practices or FPC's data processing arrangements occur. Any required amendments will be considered and approved in accordance with FPC's normal governance arrangements, ensuring continued alignment with data protection, digital compliance and AGAR requirements.

This policy forms part of FPC's wider governance framework for protecting personal data and managing information securely. It should be applied together with the IT Policy, Retention Policy, Data Roadmap and related procedures to support lawful, fair and transparent processing, proportionate digital security, effective records management and continuing compliance with the Data Protection Act 2018, UK GDPR and AGAR Assertion 10.