

HALSE PARISH COUNCIL

DATA PROTECTION POLICY

1. Purpose of the Policy

Halse Parish Council is committed to a policy of protecting the rights and privacy of individuals, including residents, staff, Councillors and volunteers. This policy outlines how the Council complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Core Data Protection Principles

The council will ensure that all personal data is:

- **Processed lawfully, fairly and transparently** in relation to individuals
- **Collected for specified, explicit and legitimate purposes** (e.g. planning consultations or public safety)
- **Adequate, relevant and limited** to what is necessary for those purposes
- **Accurate and kept up to date:** inaccurate data will be erased or rectified without delay.
- **Kept in a form that permits identification of individuals for no longer than is necessary.**
- **Processed securely** using appropriate technical or organisational measures to protect against unauthorised processing, loss or damage.

3. Roles & Responsibilities

- **The Council:** Holds overall responsibility as the Data Controller
- **The Parish Clerk:** Acts as the Council's Data Protection Lead. In accordance with Section 7(3) of the Data Protection Act 2018, the Council is exempt from the requirement to appoint a formal Data Protection Officer, but retains full accountability as Data Controller.
- **Councillors and staff:** Must handle all personal data in accordance with this policy and use official Council communication channels at all times.

4. Lawful Bases for Processing

The Council primarily processes data under the following legal frameworks:

- **Public Task:** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation (e.g. employment law, financial auditing).
- **Consent:** Where no other legal basis applies, clear and explicit consent will be sought from the individual (and can be withdrawn at any time).

5. Access and Rights (Subject Access Requests)

Individuals have the right to access their personal data held by the Council.

- Requests must be made in writing to the Parish Clerk.
- The Council will provide the information free of charge within one calendar month.
- Individuals also hold the right to rectifications erasure ('right to be forgotten'), and restriction of processing under specific legal conditions.

6. Data Security and Storage

- **Digital Files:** All electronic personal data must be stored securely on password protected devices. Passwords must be updated regularly.
- **Physical Files:** Paper records containing personal data must be stored in locked filing cabinets accessible only to authorised personnel.
- **Emails:** All Council business must be conducted via official email addresses. Personal email accounts must never be used to handle resident or staff data.

7. Data Breaches

A personal data breach is any security incident leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data.

- Any suspected data breach must be reported immediately to the Parish Clerk.
- If a breach is likely to result in a risk to the rights of freedoms of individuals, the Clerk will inform all Councillors and notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

8. Policy Review

This policy will be reviewed annually by Halse Parish Council to ensure ongoing compliance with updated legislation and regulatory guidance.

Adopted: 16 September 2026

Next Review date: September 2027