Salt and Enson Parish Council

Data Protection Policy

1. Introduction

Salt and Enson Parish Council is committed to protecting the privacy of individuals and handling personal data in a lawful, fair and transparent manner. This policy explains how the Council complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all Councilors, the Clerk/Responsible Financial Officer (RFO), employees, contractors and any other person processing personal data on behalf of the Council.

2. Definitions

- Personal Data: Any information relating to an identified or identifiable living individual.
- Special Category Data: Personal data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, or data concerning a person's sex life or sexual orientation.
- Processing: Any operation performed on personal data, including collection, storage, use, disclosure or deletion.
- Data Subject: The individual to whom the personal data relates.

3. Data Controller

Salt and Enson Parish Council is the Data Controller for the purposes of data protection legislation.

Contact details:
The Clerk to the Council – Nikola Evans
clerk@saltandensonparishcouncil.co.uk – 07388 326259 – PO Box 8033 Rugeley Staffordshire WS15 9GW

4. Data Protection Principles

The Council will ensure that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Kept for no longer than necessary

- Processed securely

The Council is accountable for demonstrating compliance with these principles.

5. Lawful Bases for Processing

The Council processes personal data under the following lawful bases: - Legal obligation - Public task - Contract - Consent (where appropriate)

Special category data will only be processed where an additional lawful condition applies.

6. Types of Personal Data Processed

The Council may process the following types of personal data: - Names, addresses, email addresses and telephone numbers - Employment and payroll information - Councilor contact details - Correspondence with residents - Complaints and enquiries - Financial information where required

7. How Personal Data is Collected

Personal data may be collected through: - Direct contact with individuals (email, letter, phone) - Council meetings and correspondence - Online forms or the Council website - Third parties where lawful and appropriate

8. Data Storage and Security

The Council will take appropriate technical and organisational measures to protect personal data, including: - Secure storage of paper records - Password-protected and encrypted electronic systems - Restricted access to personal data - Regular review of security arrangements

Personal data must not be stored on unencrypted personal devices.

9. Data Sharing

Personal data will only be shared where: - There is a legal requirement to do so - It is necessary for the performance of a public task - The individual has given consent

Data sharing will be limited to what is necessary and appropriate safeguards will be in place.

10. Data Retention

Personal data will be retained only for as long as necessary in accordance with the Council's Retention Schedule. Data will be securely deleted or destroyed when no longer required.

11. Individual Rights

Individuals have the following rights under data protection legislation: - The right to be informed - The right of access (Subject Access Requests) - The right to rectification - The right to erasure (where applicable) - The right to restrict processing - The right to data portability (where applicable) - The right to object

Requests must be made in writing to the Clerk and will be responded to within one month.

12. Subject Access Requests (SARs)

Subject Access Requests must be submitted in writing. The Clerk will: - Verify the identity of the requester - Respond within one calendar month - Provide information free of charge unless requests are manifestly unfounded or excessive

13. Data Breaches

Any actual or suspected data breach must be reported immediately to the Clerk.

The Clerk will: - Record the breach - Assess the risk to individuals - Report the breach to the Information Commissioner's Office (ICO) within 72 hours where required - Notify affected individuals where appropriate

14. Training and Awareness

All Councilors and staff will receive appropriate data protection training and guidance to ensure compliance with this policy.

15. Review of Policy

This policy will be reviewed at least every two years, or sooner if required by changes in legislation or guidance.

Adopted by Salt and Enson Parish Council: 2nd September 2027

Review date: May 2027