ALWOODLEY PARISH COUNCIL

INFORMATION AND DATA PROTECTION POLICY

1. Purpose

Alwoodley Parish Council ("the Council") recognises its responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) to ensure that personal data it holds is processed lawfully, fairly and securely. This policy sets out how the Council will manage the collection, storage, use and disposal of personal and special-category data, in accordance with legal requirements, guidance and best practice.

2. Scope

This policy applies to all Councillors, the Clerk, RFO, employees, volunteers, contractors and any other persons acting on behalf of the Council who process personal data on its behalf. It covers all personal data held in paper and electronic format, including correspondence, e-mail, video/audio recordings (including CCTV if applicable), photographs and any other relevant format.

3. Legal Framework & Guidance

This policy is based on and takes into account:

- UK GDPR (as retained in UK law) and the DPA 2018 ("Data Protection Legislation")
- The guidance issued by the Information Commissioner's Office (ICO)
- The Practitioners' Guide 2025 Addendum (Smaller Authorities) – assertion on digital and data compliance. (nalc.gov.uk)

4. Data Protection Principles

The Council will adhere to the following data protection principles (UK GDPR Article 5):

- Personal data shall be processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to erase or rectify inaccurate data without delay.
- Retained only for as long as necessary.

- Processed in a manner that ensures appropriate security of the personal data.

5. Roles & Responsibilities

- **Clerk**: Acts as the Council's *Data Protection Lead* responsible for implementation of this policy, monitoring compliance, dealing with subject access requests (SARs) and data breaches, and providing advice and training.
- **Councillors, staff and volunteers**: Must ensure that they:
    - follow this policy and associated procedures;
    - complete any required training;
    - report any data security incident or breach.
- **Council**: Oversees this policy, reviews it annually and ensures resources for compliance.

6. Lawful Bases for Processing

The Council will only process personal data where one or more lawful bases under UK GDPR applies, including but not limited to:

- **Legal obligation** (e.g., payroll, pension, audit)
- **Public task / public interest** (e.g., provision of local services)
- **Contract** (e.g., employment contract)
  Where special-category data is processed (UK GDPR Article 9), an additional condition will apply, for example: explicit consent or that it is necessary for social protection or safeguarding.

7. Data Audit, Records of Processing & Retention

- The Clerk will maintain a Register of Processing Activities (recording categories of personal data, purpose, lawful basis, retention period etc.) in line with ICO guidance.
- The Council will adopt a Records Retention & Disposal Policy which sets retention periods for all types of records in accordance with legal, audit and business needs.
- Personal data will be safely disposed of when no longer needed (paper shredded, digital files securely deleted).

8. Data Security & Technical Measures

The Council will apply appropriate technical and organisational measures to ensure security of personal data, including but not limited to:

- Secure servers, password-protected devices, encryption where appropriate
- Access control, backups, network security, regular updates
- Secure transfer of data, especially if stored or processed in the cloud or outside the UK (see ICO guidance)
- Physical security of paper records and secure disposal of devices.

9. Subject Access Requests (SARs) & Data Subject Rights

Individuals have rights under UK GDPR including: access, rectification, erasure, restriction, data portability and objection. The Council will implement a **Subject Access Request Procedure** to respond within the statutory timescale (usually one month). Fees will not be charged except as permitted by the DPA 2018.

10. Data Breach & Incident Response

- The Council will adopt a **Data Breach Response Plan** which identifies the steps to be taken in the event of a personal data breach (loss, theft, unauthorised access).
- The Clerk shall notify the ICO if required by law (typically where the breach is likely to result in risk to individuals' rights or freedoms) and inform affected data subjects where necessary.
- A record of all breaches will be maintained.

11. Third-Party Processors & Contracts

When engaging third-party suppliers who process personal data on behalf of the Council (e.g., payroll provider, website host, cloud storage), the Council shall ensure:

- A written contract or agreement in place including data protection obligations (ICO guidance & NALC toolkit)
- Due diligence on the supplier's data security arrangements
- Review of contract terms and audit rights.

12. Privacy Notices & Transparency

The Council will publish **Privacy Notices** for all data-processing activities which clearly set out: what data is processed, why, lawful basis, retention periods, rights of the data subject and contact details. These will be published on the Council website and

updated as necessary. The Council will comply with the transparency obligations in the Transparency Code for Smaller Authorities.

13. Training & Awareness

The Council will provide appropriate training and awareness for all Councillors, staff and volunteers on their data-protection responsibilities. The Clerk will maintain records of training. The Council will review and monitor compliance through periodic audits.

14. Monitoring, Audit & Review

- The Clerk will conduct periodic internal audits of data-protection compliance (e.g., data audits, security checks).
- The Council will review this policy annually at the Annual Meeting and whenever there is a material change in law, technology or structure.
- The next formal review date is November 30, 2026

15. Policy Publication & Version Control

This policy will be published on the Council's website and is freely available to members of the public. A master copy is held by the Clerk.

Adopted: 3rd November 2025
Next Review: November 2027