WINDLESHAM PARISH COUNCIL

DATA PROTECTION POLICY (November 2025 Edition)

Table of Contents

Version & Date | Amendments made

V4.0–251010 | Reviewed and updated to comply with UK GDPR, DPA 2018, and Data Use and Access Act 2025. Incorporates current ICO guidance, seven data protection principles, lawful bases, breach notification procedure, and new data rights.

1. Introduction

1.1 Windlesham Parish Council ("the Council") collects and processes personal data relating to employees, councillors, contractors, residents, service users, and other individuals ("data subjects") in the course of its operations.

1.2 This policy sets out how the Council complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data Use and Access Act 2025 (DUAA 2025).

1.3 The Council is committed to ensuring that personal data is handled lawfully, transparently, and securely, and that individuals' privacy rights are always respected and adhered to.

2. Scope and Purpose

2.1 This policy applies to all personal data held by the Council in any format, including electronic, paper, audio, and video data.

2.2 It applies to all councillors, employees, agency staff, contractors, volunteers, and any third parties who process personal data on behalf of the Council.

2.3 The purpose of this policy is to ensure that the Council processes data fairly, lawfully, and transparently; maintains accountability; and protects the privacy and security of all individuals whose data it holds.

3. Data Protection Principles

The Council adheres to the seven data protection principles set out in Article 5 of the UK GDPR. Personal data shall be:

1. Lawfulness, fairness and transparency – processed lawfully, fairly, and in a transparent manner.

2. Purpose limitation – collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

3. Data minimisation – adequate, relevant, and limited to what is necessary.

4. Accuracy – accurate and, where necessary, kept up to date.

5. Storage limitation – kept no longer than necessary.

6. Integrity and confidentiality – processed securely using appropriate technical and organisational measures.

7. Accountability – the Council is responsible for, and must be able to demonstrate, compliance with these principles.

4. Lawful Bases for Processing

4.1 The Council will ensure that every instance of data processing has a lawful basis under Article 6 of the UK GDPR, including consent, contract, legal obligation, vital interests, public task, and legitimate interests (rarely applicable to public authorities).

4.2 Where special category or criminal offence data is processed, the Council will identify the relevant condition under Articles 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018.

4.3 The lawful basis for each processing activity will be documented in the Council's Record of Processing Activities (ROPA).

5. Roles and Responsibilities

5.1 The Council is the Data Controller for all personal data it processes.

5.2 The Council has appointed GDPR-info Ltd as its independent Data Protection Officer (DPO). The DPO is responsible for monitoring compliance, advising on DPIAs, and acting as the point of contact for the ICO.

5.3 All staff, councillors, and contractors must complete annual data protection training, follow this policy, and report any suspected data breaches immediately.

6. Storage, Security, and Retention

6.1 Personal data shall be stored securely using password-protected and access-controlled systems, with encryption and regular backups.

6.2 Sensitive personal data shall be restricted to authorised personnel and stored in secure, encrypted areas (e.g., restricted SharePoint folders or locked cabinets).

6.3 The Council's Document Retention Schedule sets out retention periods. Data will be securely deleted or destroyed when no longer required.

6.4 Under the DUAA 2025, data shared with third parties will include metadata and provenance information to ensure transparency and accountability.

7. Data Subject Rights

Individuals have the following rights under the UK GDPR and DUAA 2025: access, rectification, erasure, restriction, portability, objection, automated decision-making review, and transparency of data use.

7.1 Subject Access Requests (SARs) should be made in writing to the Clerk or DPO.

7.2 The Council will respond within one month, extendable by two months for complex requests.

7.3 If a request is manifestly unfounded or excessive, the Council may charge a reasonable fee or refuse the request with reasons.

8. Data Sharing and Third-Party Access

8.1 The Council may share personal data with public bodies, contractors, or service providers where necessary to perform its functions or comply with legal obligations.

8.2 All third-party data sharing will be governed by a Data Sharing Agreement or Data Processing Agreement compliant with UK GDPR, DPA 2018, and DUAA 2025.

8.3 The Council will publish transparency information on any regular or large-scale data sharing under the DUAA 2025 Public Data Use Register.

9. Automated Decision-Making and AI Use

9.1 The Council will ensure that no automated decision-making or profiling takes place without a lawful basis under Article 22 UK GDPR and appropriate safeguards.

9.2 In line with the DUAA 2025, any use of AI or algorithmic systems will be documented in the Council's Algorithmic Transparency Record, subject to fairness audits, and explained to affected individuals.

10. Breach Management and Reporting

10.1 Any personal data breach must be reported immediately to the DPO and Clerk.

10.2 The DPO will assess the breach. If it poses a risk to individuals' rights and freedoms, the ICO will be notified within 72 hours, and affected individuals informed without undue delay.

10.3 All breaches will be logged in the Data Breach Register.

10.4 Failure to comply may result in disciplinary action or legal proceedings.

11. Review and Updates

11.1 This policy will be reviewed annually or sooner if legislation, ICO guidance, or Council operations change.

11.2 The next scheduled review date is October 2026.

Contact

For questions or to exercise your rights under this policy, contact:

The Clerk
Windlesham Parish Council
Email: [Insert contact email]
Or the Data Protection Officer (GDPR-info Ltd) via the Clerk