Windlesham Parish Council

Breach Notification Policy *(DUAA 2025 Compliant)*

Version: 1.2-25 Approved:25th November 2025

1. Scope

- This procedure applies under the UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025.
- The Council identifies whether it acts as Data Controller or Data Processor (DPO) for each activity. Joint controllerships will be documented.
- This policy also ensures compliance with DUAA 2025 requirements on accountability, audit, and complaints handling.
- As well as written and paper records it also applies to electronic data held on Council IT servers and electronic devices, including those managed by third parties.
- The Council risks prosecution and fines for non-compliance, so adherence at all times is essential by the Council in its activities and records.

2. Responsibilities

- All councillors, staff, contractors, and third parties must follow this procedure..
- The Data Protection Officer (GDPR-Info Ltd) provides advice and liaises with the ICO.
- All personnel and Councilors complete annual data protection and breach-response training.

3. Processor to Controller Notification

- Processors report breaches without undue delay to the Clerk and DPO via secure, encrypted communication.
- Receipt must be confirmed within 24 hours.
- The Clerk logs all breaches in the Breach Register, retained for five years.

4. Controller to Supervisory Authority (ICO)

- The Clerk ensures **notifiable** breaches are reported to the ICO via the DPO within 72 hours where feasible.
- Notification includes nature of breach, categories affected, lawful basis, contact details, consequences, and mitigation.
- Delays beyond 72 hours must be justified and recorded.
- All breach correspondence is retained for five years.

5. Controller to Data Subject

- Where a breach poses high risk, affected individuals will be informed promptly in clear, plain language.
- Alternative accessible formats are available if required.
- If direct contact is disproportionate, a public notice may be issued, with rationale recorded and DPO approval obtained.

6. Complaints Handling (DUAA 2025 Requirement)

- Data subjects may submit complaints in writing to the Clerk.
- Complaints are acknowledged within 30 days and handled without undue delay.
- All complaints and responses are logged for audit.

7. Accountability, Audit, and Transparency

- Full audit trail of breaches, notifications, and decisions is retained for five years.
- An annual breach simulation tests readiness.
- A policy summary and contact details are published online for transparency.

8. Review

- This policy is reviewed annually or following legislative change, including updates to the DUAA 2025.