# Quatt Malvern Parish Council

## Explanatory letter — Data Protection Policy and General Privacy Notice

Dear Bill,

Thank you for sending over the draft Data Protection Policy and General Privacy Notice. I have prepared a proposed replacement, keeping the approach practical for a small parish council and avoiding obligations which may not reflect the Council's actual activities.

As with the previous policies, these are suggestions to help the Council adopt a document that is accurate and usable, rather than criticism of the work already undertaken.

## Principal changes and reasons

### 1. Updated legal framework

The draft referred generally to "GDPR". The replacement refers to the UK GDPR, Data Protection Act 2018 and amendments made by the Data (Use and Access) Act 2025.

### 2. Clearer distinction between policy and privacy notice

The original combined internal instructions and information for residents. The replacement retains one document but separates the two functions into Part A and Part B.

### 3. Correct lawful bases

The draft treated the Council's statutory functions largely as "legal obligation". Public task and legal obligation are separate bases; the replacement distinguishes them and gives a practical summary, subject to confirmation of actual activities.

### 4. Remove speculative personal information categories

The original included genetic, biometric, sexual-life, criminal-conviction and other categories, together with CCTV and credit reference agencies. These should not be presented as routine Council activities unless they genuinely occur.

### 5. Appropriate retention arrangements

The original suggested eight years for financial records. A documented retention schedule, based on the actual type of record and relevant requirements, is more defensible than a blanket period.

### 6. UK international transfer wording

The original referred to the EEA and EU-approved contracts. The replacement uses UK international transfer terminology and asks the Clerk to verify the actual email and cloud arrangements.

### 7. Individual rights

The replacement makes clear that rights are conditional and that erasure or portability may not apply to public-task processing. It also links to the separate Subject Access Policy.

### 8. Data protection complaints

A clear complaints route is now required. The Council must facilitate complaints, acknowledge them within 30 days, investigate appropriately and communicate an outcome without undue delay.

### 9. Breach handling

The draft broadly covered breach reporting. The replacement distinguishes recording all breaches from reporting those meeting the ICO risk threshold, and provides a practical escalation route.

### 10. Roles and security

The Council is the controller; the Clerk coordinates compliance. The replacement links to the Council's new IT Policy and its dedicated .gov.uk email arrangements.

## Practical checks before adoption or publication

- Confirm the Clerk's current postal address, official email and telephone number; I have deliberately left the email and telephone for confirmation.
- Check that the descriptions of Council activities and recipients match what the Council actually does; add any genuine activities not covered.
- Approve a simple records retention schedule, even if it is initially a short working table.
- Confirm the Council's cloud/email provider, whether any restricted international transfers occur and the safeguards in place.
- Ensure the website provides an easy route to make a data protection complaint, including an electronic method.
- Confirm who will handle a complaint involving the Clerk and how records will be kept confidential.
- Check that this notice and the separate Subject Access and IT Policies use consistent terminology and contact details.

## Suggested approach

I would suggest treating the enclosed document as the basis for adoption once the factual checks above have been completed. It should then be published on the Council website and reviewed annually. I have intentionally avoided making the policy unnecessarily elaborate: the key is that the Council can demonstrate it follows the procedures it adopts.

I hope this is helpful. I am very happy to discuss any of the changes before the papers go to Council.

Kind regards,



Steve Jones

Internal Auditor

## Official guidance consulted

ICO — Data protection complaints: https://ico.org.uk/for-organisations/how-to-deal-with-data-protection-complaints/

ICO — Public task lawful basis: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/public-task/

ICO — Data (Use and Access) Act 2025: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/