Data Protection Compliance Checklist for Parish Councils

1. Governance & Accountability

A Data Protection Policy is adopted and regularly reviewed by Council.

The Council has appointed a Data Protection Officer (DPO) or confirmed exemption.

All councillors and staff have received basic GDPR training.

A data protection risk register or record of key compliance activities is maintained.

2. Data Inventory & Lawful Basis

An Information Asset Register or Record of Processing Activities (ROPA) is in place.

The lawful basis for all data processing (e.g., consent, legal obligation, public task) is clearly documented.

The Council only collects data necessary for its purpose (data minimisation principle).

3. Security & Access Controls

Personal data is stored securely (e.g. password-protected computers, locked cabinets).

Access to data is restricted to authorised personnel only.

Councillors and staff do not use personal email accounts for council business.

4. Privacy Notices

A Privacy Notice is published on the Council's website and reviewed annually.

The notice explains the Council's data collection, use, retention, and rights.

5. Data Retention & Disposal

A Retention Policy outlines how long personal data is kept.

Personal data is securely deleted or destroyed when no longer needed.

6. Individual Rights

The Council has procedures to respond to Subject Access Requests (SARs) within 1 month.

Procedures exist for handling requests for:

Data correction

Data erasure (where applicable)

Objections or restrictions to processing

7. Data Breaches

A Data Breach Procedure is in place and staff know how to report incidents.

All breaches are recorded, and those affecting rights/freedoms are reported to the ICO within 72 hours.

8. Sharing & Third Parties

Data sharing with contractors (e.g., payroll, website hosting) is covered by data processing agreements.

The Council ensures third parties are GDPR-compliant.

9. Annual Review

The Clerk or DPO conducts an annual review of all policies and practices.

Updates are made in line with guidance from the Information Commissioner's Office (ICO).

Supporting Policies/Docs You Should Have:

Policy	Reviewed Annually?
Data Protection Policy	☑
Privacy Notice	☑
Retention & Disposal Policy	☑
Data Breach Procedure	☑
Information Asset Register	☑

Governance & Accountability

Checkpoint	How to Achieve
Adopt a Data Protection Policy	Use a model policy from NALC or SLCC. Tailor it to your council's size and activities. Review and adopt it annually at a Full Council meeting.
Appoint a Data Protection Officer (DPO)	Councils may be exempt, but it's best practice to nominate the Clerk or a shared service via your District or County Council.
Staff & Councillor Training	Arrange basic GDPR training via SLCC, your CALC, or free ICO resources. Keep attendance records.
Maintain a Data Protection Risk Register	Create a simple spreadsheet identifying data risks (e.g., unauthorised access, accidental loss), likelihood, and mitigation steps.

Data Inventory & Lawful Basis

Checkpoint	How to Achieve
Create an Information Asset Register (IAR)	List all data held (e.g., payroll, allotment tenants, email contacts), where it's stored, who has access, and why it's kept.
Document Lawful Basis	For each data set in the IAR, assign one lawful basis (e.g., legal obligation for payroll; consent for newsletters). Refer to Article 6 of UK GDPR.
Apply Data Minimisation	Only collect what is essential. E.g., don't ask for date of birth if age is not relevant to the service. Regularly audit forms and registers.

Security & Access Controls

Checkpoint	How to Achieve

Secure Data Storage	Use password protection for electronic files. Lock physical records in cabinets. Use council-owned devices where possible.
Limit Access	Ensure only those who need access (e.g., Clerk, RFO) have it. Create separate folders for confidential data.
Avoid Personal Email Use	Set up official emails (e.g., clerk@yourcouncil.gov.uk). Train councillors to use these accounts for all council business.

Privacy Notices

Checkpoint	How to Achieve
Publish a Privacy Notice	Use the ICO's privacy notice checklist and a NALC model to create one. Publish it on the website and signpost it in correspondence and forms.
Explain Data Use Clearly	State what you collect, why, how long you keep it, who you share it with, and the rights of data subjects.

Data Retention & Disposal

Checkpoint	How to Achieve
Adopt a Retention Policy	Base this on the NALC's Legal Topic Note (LTN 40) and SLCC's guidance. Link retention periods to document types (e.g., minutes = permanent; job applications = 6 months).
Secure Disposal	Shred paper records. Delete digital files from all storage areas (e.g., Dropbox, USB, hard drives). Keep a log of what was destroyed and when.

Individual Rights

Checkpoint	How to Achieve
SAR Procedure	Create a simple flowchart with deadlines (respond within 1 month). Template response letters are available from the ICO.
Process Other Rights	Include checklists to ensure you handle correction requests, objections, or erasure properly. Seek advice from the DPO if unsure.

Data Breaches

Checkpoint	How to Achieve
Create a Breach Policy	Use NALC or ICO templates. Include who to notify (ICO, data subject), when, and how. Publish the policy or include it in the main Data Protection Policy.
Keep a Breach Log	Even if the breach is minor, record it. Use a spreadsheet noting date, description, who was informed, and lessons learned.

Sharing & Third Parties

Checkpoint	How to Achieve
Data Sharing Agreements	When using payroll services, email providers, or IT support, ensure a contract or agreement includes data protection clauses.
Check Their GDPR Compliance	Ask suppliers for their privacy policy or ICO registration number. Use only reputable providers for cloud or storage solutions.

Annual Review

Checkpoint	How to Achieve
Annual Policy Review	Add this to your April or May agenda. Review all data policies, asset register, breach log, and training records. Make updates where needed.
Monitor ICO Updates	Sign up to the ICO newsletter. Watch for updates relevant to councils (they’re usually highlighted by SLCC and NALC too).