PORLOCK PARISH COUNCIL
GDPR & DATA PROTECTION
DATA AUDIT CHECKLIST

Area	Action	Completed
Preparation	Assign a lead officer for the data audit (e.g., Clerk/RFO).	
	Define scope: all council data including digital and paper.	
	Gather existing policies (privacy notice, retention policy, IT policy).	
Identify Data Locations	List all systems where council data is stored (email, cloud drives, finance software).	
	Identify paper records (filing cabinets, archives).	
	Include councillor devices if council business data is stored there.	
Identify Data Types	Record what personal data is held in each system.	
	Identify the data subjects (residents, staff, contractors, allotment holders).	
	Note if sensitive or special category data is present.	
Legal Basis	Identify the legal basis for processing (public task, contract, legal obligation, consent).	
	Check privacy notices reflect the processing activities.	
Access & Permissions	Document who has access to each dataset.	
	Confirm access is limited to those who need it.	
	Remove unnecessary permissions.	
Security Review	Check password protection on files and systems.	
	Confirm backups are in place.	
	Ensure paper records are stored securely.	
Retention & Deletion	Check how long data is retained.	
	Compare with recommended retention periods.	
	Delete or archive data no longer required.	
Risks & Improvements	Identify risks such as duplicated data or unsecured storage.	
	Note any required policy or system improvements.	
Create Data Asset Register	Compile all findings into a Data Asset Register spreadsheet.	
	Assign a data owner for each dataset.	
Report & Action Plan	Summarise findings to the council.	
	Create an action plan for improvements.	
	Schedule the next audit (recommended annually).	

DRAFT