

Pirbright Parish Council – Data Audit Report

Date Completed: 3rd November 2025
Clerk/Responsible Officer: Helen Myers
Reviewed By: Full Council 11th November 2025

1. Overview

This data audit sets out how Pirbright Parish Council processes personal data in the course of its duties and functions. It is designed to ensure compliance with the UK GDPR and Data Protection Act 2018, promote transparency, and support accountability.

2. Data Inventory Table

Data Category	What Personal Data?	Who It Relates To	Purpose	Lawful Basis	How It's Collected	How It's Stored	Retention Period	Shared With
Council Minutes & Agendas	Names, roles, public comments	Councillors, public	Governance, public record	Legal Obligation	Directly at meetings or submissions	Website, Secure cloud storage and hard copy	Indefinite (archival)	Public via website
Planning Comments	Name, address, comment content	Residents	Responding to planning applications	Public Task	Email	Secure cloud storage, hard copy	6 years	GBC Planning
Hall Hire and Pavilion Hire Records	Name, contact details, payment info	Hirers	Booking and invoicing	Contract	Hire form/email	Secure cloud storage	6 years (financial)	None
Staff Records	Name, address, payroll data, appraisals	Employees	Employment	Legal Obligation & Contract	Directly from staff	Secure cloud storage, locked file	6 years post-employment	Payroll provider, HMRC, Auditor
Email Enquiries	Name, contact info, content	General public	Responding to queries	Legitimate Interest	Email	secure cloud storage/email server	1 year	Councillors, GBC and SCC if necessary to resolve query
CCTV (if applicable)	Video footage	Visitors to council property	Security	Legitimate Interest	CCTV system	DVR	Max 30 days unless incident	Police (if required)
Finance	Name, Payment details	Staff, residents and contractors	To make and receive payments	Legitimate Interest	Directly from person or via the bank	Secure cloud storage, hard copy	Until no longer needed or 6 years	Councillors for authorisation and monitoring. Auditors

3. Data Processors (External Parties)

Processor	Purpose	Data Shared	DPA in Place? (Data Processing Agreement)	Other info
Payroll Provider - Payroll	Monthly payroll	Employee details	Yes and in place until terminated	
HMRC	Statutory reporting	Employee pay/tax	No DPA required. The Council shares employee data with HMRC for payroll, tax and pension purposes. HMRC acts as a data controller under relevant UK tax legislation. Article 6(1)(c) – Legal obligation	
Website Host - Spanglefish	Council website	Public documents	Yes and in place until terminated	
Email Provider (e.g. Outlook/Microsoft)	Communication	Emails	www.pirbright-pc.gov.uk	
External Auditors - PKF Littlejohn LLP	Financial audit	Invoices, pay, contracts	Data shared with the appointed external auditor (PKF Littlejohn LLP) as part of statutory audit requirements under the Local Audit and Accountability Act 2014. PKF Littlejohn acts as an independent data controller. PKF Littlejohn publishes their own privacy notice (see below)	https://www.pkf-l.com/data-protection-privacy-notice/
Internal Auditor - Mulberry LAS	Internal audit of council governance, financial	Including access to payroll, personnel, and	Yes and in place until terminated	
ISS	Computer backup and support	All electronic information	Yes and in place until terminated	
Guildford Borough Council	Governance, planning, assistance with queries	Contact details - names, addresses, emails	dpo@guildford.gov.uk Yes and in place until terminated	
Surrey County Council	Assistance with resident queries	Contact details - names, addresses, emails	https://www.surreycc.gov.uk/council-and-democracy/your-privacy/corporate-privacy-notice	
Lloyds Bank, Nationwide, Boom and Unity Bank	Council banking	Account names, numbers, councillors and staff identity documents and personal identification details	Banks act as data controllers, deciding how and why they process personal data (e.g., identity checks, account management). The Council provides necessary personal data (e.g., signatory details) for the bank's lawful purposes, not under the Council's instruction. Therefore, under UK GDPR, no Data Processing Agreement is required. The council will share only necessary data, keep a record of what is shared and why and use banks with appropriate data protection measures.	
SignRequest	Authorisation Software	Contact details - names, addresses, emails , bank account details	Yes and in place until terminated. GDPR compliant. Restricting who can access signed documents and personal data will minimise the risk of a data breach. Examples of access controls include role-based access management, multi-factor authentication and logging and monitoring of user activity. This protects data and strengthens accountability. The Clerk attends regular training on GDPR. PPC are members of the ICO. SignRequest meets all GDPR requirements especially in relation to using a robust audit trail, consent logs and encryption standards.	

4. Security Measures

- Password-protected cloud storage and gov.uk email accounts
- Daily backups
- Paper files stored in locked cabinet/locked room
- Anti-virus and firewall protection
- Limited access to personal data internally
- Regular reviews of IT and data handling procedures
- E-Signature software which is fully GDPR compliant