Great Tey Parish Council – Data Protection Roadmap & Data Inventory

Introduction and Purpose:

Great Tey Parish Council acknowledges its statutory responsibilities as a data controller under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The Council is committed to processing personal data lawfully, fairly and transparently, and to ensuring that appropriate technical and organisational measures are in place to protect personal data in line with the principles set out by the Information Commissioner's Office (ICO).

To support this commitment and to demonstrate compliance with the UK GDPR accountability principle (Article 5(2)), the Council maintains both a Data Protection Road Map and a Data Inventory. These documents form part of the Council's wider governance framework and internal control environment.

The Data Protection Road Map sets out a structured and proportionate approach to achieving and maintaining compliance with data protection legislation. It identifies the actions required to implement, monitor, review and improve the Council's data protection arrangements, including policies, procedures, training, risk management and information security controls. The Road Map enables the Council to plan improvements over time, to evidence ongoing compliance, and to respond appropriately to changes in legislation, guidance or the Council's activities, in accordance with ICO and National Association of Local Councils (NALC) guidance.

The Data Inventory records the personal data processed by the Council and includes details of the purpose for processing, the lawful basis relied upon, categories of data subjects and personal data, retention periods, data sharing arrangements, and the security measures in place. This supports compliance with Article 30 of the UK GDPR and enables the Council to manage data protection risks effectively, respond to data subject rights requests, and ensure that personal data is not retained or processed unnecessarily.

Together, the Data Protection Road Map and Data Inventory provide documented evidence that the Council understands its data protection obligations and has appropriate arrangements in place to meet them. They support compliance with the UK GDPR principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality. The documents are reviewed periodically and updated as required to ensure they remain accurate and effective.

The maintenance and review of these documents also support the Council's assertions under the Annual Governance and Accountability Return (AGAR), particularly in demonstrating that the Council:

- maintains an adequate system of internal control;
- takes reasonable steps to ensure compliance with laws and regulations;
- identifies and manages risks appropriately; and
- applies proper governance and accountability arrangements.

Great Tey Parish Council

By maintaining a Data Protection Road Map and Data Inventory, the Parish Council provides assurance to councillors, residents, regulators and auditors that personal data is managed responsibly, proportionately and in line with legal and best practice requirements.

Risk Level Colour Key

- High (Red): Sensitive personal data that could cause significant harm if lost, stolen, or misused (e.g., financial, DBS, staff HR data).
- Medium (Orange): Personal data that could cause moderate impact if compromised (e.g., councillors' personal info, communications).
- Low (Green): Minimal risk if lost or misused; mostly general or non-sensitive data (e.g., training logs, general social media info).

Category	Personal Data Held	Purpose / Use	Legal Basis	Storage Location	Retention Period	Access / Roles	Security Measures	Risk Level	Notes / Additional Considerations
Residents	Name, address, email, phone, payment info, correspondence	Service provision, payments, newsletter, correspondence	Legal obligation; Consent	Council server, encrypted cloud, paper files in locked cabinets	Financial: 6–7 years; Correspondence: 1–3 years	Clerk, councillors (as needed), authorised volunteers	Password-protected systems, encrypted emails, locked cabinets, access on a need-to-know basis	High (Red)	Includes online forms, email, social media messages. Consent required for newsletters. Payment info is sensitive.
Staff	Name, address, email, phone, bank details, NI number, employment records, appraisals, leave records, training records	HR management, payroll, performance management, training	Legal obligation; Contractual necessity	HR system, payroll software, paper personnel files	Employment duration + 6 years	Clerk, HR adviser, payroll provider	Encrypted files, restricted access, secure cloud storage, locked filing cabinets	High (Red)	Includes digital communications, performance notes. Must comply with GDPR.
Councillors	Name, address, email, phone, term of office, committee membership, declarations of interests	Governance, council communications, public record keeping	Legal obligation; Public task	Council server, secure email, paper records in locked cabinets	Term + 5 years	Clerk, council chair, authorised staff	Password-protected systems, secure email, limited access	Medium (Orange)	Include social media engagement linked to official council business.
Volunteers	Name, address, email, phone, emergency contact, role, DBS info (if applicable)	Volunteer management, task allocation, insurance, safeguarding	Consent; Legal obligation (for DBS checks)	Secure council server, locked cabinets	Duration of involvement + 2 years	Clerk, project leads	Password-protected records, locked cabinets,	High (Red)	Minimise personal data storage for non-DBS volunteers. Training records securely stored.

Category	Personal Data Held	Purpose / Use	Legal Basis	Storage Location	Retention Period	Access / Roles	Security Measures	Risk Level	Notes / Additional Considerations
							restricted access		
Contractors / Suppliers	Name, company, email, phone, address, contract terms, payment info	Contract management, service delivery, payments	Contractual necessity; Legal obligation	Council server, secure cloud, paper files	Contract + 6 years	Clerk, finance officer	Encrypted systems, locked cabinets, limited access	Medium (Orange)	Includes invoices, work records. Ensure secure banking info transmission.
Social Media / Communications	Posts, messages, emails, website contact forms, newsletters, complaints	Public engagement, information dissemination, consultation	Consent; Legitimate interest	Secure council email, social media accounts, website CMS	1–3 years depending on purpose	Clerk, communications officer	Secure login, MFA, encrypted email, monitoring of access	Medium (Orange)	Include monitoring for GDPR compliance, avoid posting personal data without consent.
IT Logs / Systems	Login records, system usage logs, email logs, incident reports	IT security, compliance, audit, incident investigation	Legitimate interest; Legal obligation	Secure server, IT provider logs	1 year or as per IT policy	IT provider, clerk, authorised IT staff	Access control, encryption, MFA, regular backups	Medium (Orange)	Include phishing and cyber awareness logs, password management, audit trails.
Phishing / Cyber Awareness Records	Training completion records, incident reports, suspicious email logs	Staff awareness, incident tracking, regulatory compliance	Legal obligation; Legitimate interest	Secure HR system, IT logs	3 years	Clerk, IT provider, HR	Restricted access, password-protected, encrypted	Low (Green)	Used for annual training reports, regulatory audits, internal awareness campaigns.
Financial / Payments (Residents, Staff, Contractors)	Bank details, payment history, invoices, receipts	Payments, accounting, auditing	Legal obligation	Secure finance system, encrypted cloud, locked cabinets	6–7 years	Clerk, finance officer, auditors	Encrypted storage, limited access, secure backups	High (Red)	Ensure PCI compliance where applicable, avoid storing unnecessary card details.
Complaints / Correspondence	Name, contact info, complaint details, investigation notes	Investigation, resolution, record keeping	Legal obligation; Legitimate interest	Secure council server, locked cabinets	3–6 years depending on severity	Clerk, relevant staff	Encrypted digital storage, locked cabinets, access on a need-to-know basis	Medium (Orange)	Ensure confidentiality, only share with authorised parties.