St. Peter the Great Parish Council

Data Protection Policy

This document explains how St Peters parish Council (Worcester) complies with the Data Protection Act (DPA) 1998. The policy uses guidance published by the Information Commissioner's Office (ICO) ico.org.uk.

Data Controller

St Peter the Great County Parish Council (Worcester) ('the Parish Council') is a Data Controller and has registered with ICO (registration reference: A1066992).

The Clerk to the Council is responsible for:

- Ensuring that the Parish Council complies with the provisions of the DPA;
- Implementation of this policy;
- Handling subject access requests in accordance with the DPA.

The Parish Council and Clerk may be contacted via the Parish Council web site: www.stpetersworcs.org.uk

Parish Councillors

This policy applies to the Parish Council and its employees. It does not apply to Council Members (Parish Councillors) who may need to register as data controllers in their own right, except where:

- The Parish Council may disclose personal information to Council Members where necessary to fulfil a council function. In such cases the Parish Councillor is subject to this policy as if they were an employee.

Data Protection Principles

It is Parish Council policy to fully comply with the Data Protection Principles defined in the DPA:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
   a) at least one of the conditions in Schedule 2 is met, and
   b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4) Personal data shall be accurate and, where necessary, kept up to date.
5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

v0/1st March 2015/ADOPTED: 30th March 2015

Personal Information Processed by the Parish Council (Principles 1-6)

The Parish Council acquires and processes personal information in the following circumstances:

General Purpose	Typical Type of Personal Information	Data Handling Policy
As a Parish Council	Member contact details. Member Disclosable Interests. Additional personal information (e.g. a photograph)	Member Declarations of Interest are required in law to be published on the web site. Personal information concerning Members may be published that is already public or with their express consent. Data is maintained only for the duration of office.
As an employer	Personal & financial details of employees and applicants	Subject to Employee Recruitment & Appointment Policy (Adopted 23/2/2015). Employee records are held by the Clerk and only Members appointed by Minuted decision of the Council where required.
Dealing with suppliers	Contact and payment details of the supplier and records relating to supplier performance	Records are held by the Clerk and only Members appointed by Minuted decision of the Council where required.
Parish magazine (Newslink) advertisers	Contact details of the advertising purchaser and records of transactions.	Records are held by the Clerk and only Members appointed by Minuted decision of the Council where required.
Dealing with data processors (e.g. Newslink editor/advertising manager)	Contact details of the advertising purchaser and records of transactions and contact details of magazine contributors.	The Clerk will verify that the data processor that is processing personal information on behalf of the Parish Council complies with the DPA.
Parish Council Web Site	The web site only contains information intended to be public. The web site includes a facility for the public to contact the Parish Council by email. The member of the public may optionally include personal contact information.	This data protection policy is published on the web site. The web site includes appropriate data protection statements.
Parish Survey	A respondent may optionally include their name and contact details to enable the Parish Council to verify that the response is valid (from a resident of the Parish) and unique.	Records are held by the Clerk and only Members appointed by Minuted decision of the Council where required.
Member of the public contacts the Parish Council (distinct from contacting a Councillor)	Name and contact details in association with the correspondence and possibly information included by the originator.	Contact to the Council is directly to the Clerk, Chairman or Vice-Chairman. The general issue may be shared with the whole Parish Council only after all personal information has been removed, unless the Clerk has express permission from the originator (and any other people cited). Records are held by the Clerk, Chairman or View-Chairman and only Members appointed by Minuted decision of the Council where required.

Personal information in possession of the Parish Council is only processed in accordance with the above table.

Sensitive Personal Information

The Parish Council does not process sensitive personal information.

Protecting Personal Information (Principle 7)

Employees and Council Members (Parish Councillors) acting on behalf of the Parish Council shall protect personal information in scope of this policy in accordance with the following:

1) Personal computers.

   Personal computers should be secured with a strong password to prevent unauthorised access to personal information should the aforementioned computer be stolen, passed on or otherwise compromised. Internet connected devices should be running anti-virus software and be protected by a suitable firewall device such as a properly configured router provided buy an Internet Service Provider.

   Where a personal computer is shared, any personal information subject to this policy processed on that computer shall be protected by password only known to the employee/Councillor (for example through the use of a separate user account or password protected files).

2) Personal mobile devices and removable storage used by the Clerk, other staff and councillors

   Councillor's mobile devices that are capable of storing personal information and/or sending and receiving email should secure those devices using a PIN or other device security facility to prevent unauthorised access to personal information should the device be stolen, passed on or otherwise compromised.

   USB drives shall not be used.

3) Physical Security of electronic and paper-based information held by the Clerk, other staff and councillor' places of residence.

   All reasonable steps to secure information in the residence should be taken. Information of a sensitive nature, including but not limited to financial documents, cheque books and banking credentials should be physically locked away in a secure manner.

4) Use of externally hosted services (email, cloud storage services)

   External services and email accounts shall be secured with a strong password to prevent access to the account from remote devices.

5) Disposal of personal information when no longer required

   Personal information stored electronically shall be deleted from the appropriate applications, including deletion from the 'Recycling Bin' and reasonable endeavours to remove all copies and backups. (Records may persist in electronic backups for long periods. These records are only accessed in exceptional circumstances and any out of data personal records shall be deleted at the point they are discovered in backup records.)

   Personal information in printed form shall be disposed of in such a way that the information cannot easily be reconstituted, for example by shredding or burning.

Personal data transfer overseas (Principle 8)

The Parish Council shall not transfer (or use suppliers/data processors that would lead to transfer) personal data to a country or territory outside the European Economic Area.