

South Marston Parish Council

General Data Protection Regulations Policy

General:

South Marston resolve to adhere to the General Data Protections Regulations as appropriate for an organisation of our size and structure. We will always build data protection into new projects as they occur.

We note that Local councils and parish meetings do not fall into the definition of a 'public authority' for the purposes of the Data Protection Act 2018. The rationale for this according to the debates in Parliament is that local councils and parish meetings will not normally be processing personal data 'on a large scale'.

Training:

All Councillors and staff should be conscious of the GDPR regulations in all they do.

We aim to provide training for all Councillors and staff that handle data and produce a briefing sheet for all those that can't.

Roles:

All roles are appointed at the Annual Meeting of the Council and will be held for 12 months, unless otherwise stated by the Council.

Data Protection Officer: As a Parish Council we are excluded from requiring to have an Data Protection Officer as we do not process personal data for regular and systematic monitoring of data subjects on a large scale, or process sensitive personal data on a large scale.

However, the Parish Council may choose to appoint a Councillor as a Data Protection Officer to provide additional support and oversight in Data Protection matters.

Data Controller: The Data Controller will always be the Clerk of South Marston Parish Council as part of their role in managing the administration of the Council. However, the Council, remains responsible for compliance with the data protection legislation.

Data held:

South Marston Parish Council holds the following data

Data subject	Processing details	Lawful reason	Type of data included	Duration & destruction
Allotment tenancy information	Collected via phone and email. Viewed by Allotment Working Group members for management of allotments.	Small Holdings and Allotments Act 1908, s23	Name, address, email, telephone numbers, payment information and history, inspection results	5 years. Deleted once no longer needed
Community News contributor	Collected via email to editor and Comms WG. Stored on secure PC	For creation of Community News	Name, email address	While interested in contributing. Removed from mailing list on request
Community News deliverer	Collected via email. Compiled in outlook group and stored on secure PC	For delivery of Community News	Name, address, email address	While interested in delivering. Removed from mailing list on request
Local resident contact information – members of working groups or similar task-limited groups.	Used by working groups or task groups.	To enable effective participation.	Name, address, email address	Deletion after completion of task or as deemed relevant to working group.
Local resident contact information – Held by Clerk	Used as residents contact Clerk with queries. Remain in outlook system until deletion of old emails.	For query management	Name, email address, query details	Deleted with old emails (2 years)
Local resident contact information – Held by Councillors	Used by Councillors to contact residents. Councillors should always be clear if residents are giving contact details to them as neighbours or as Councillors.	For query management	Name, email address, postal address, query details	Until no longer needed. Should not be held in personal mailboxes.

Subject access requests:

On receipt of a subject access request, the details will be sent to the Data Protection Officer (DPO). The DPO will liaise with the Data Controller to identify the information required and the timescale for a response. The DPO will inform the enquirer of an estimated response time (This must be within 40 days of the request being received by the Council.)

The Data Controller will produce the required information and forward to the Data Protection Officer for sharing with the enquirer. The Data Controller will record the request and information sent in the subject access request spreadsheet.

Data protection breaches:

Data breaches must be immediately reported to the Data Protection Officer, who will notify the Information Commissioners Office within 72 hours where there is significant risk to those whose data has been breached.

The Data Protection Officer will record the details of the breach along with details of actions taken. The Data Protection Officer and Data Controller are responsible for dealing with any data breaches which may occur, outlining a response plan and make recommendations to the Council how to resolve and prevent further breaches.

Where appropriate, those affected by the breach should be informed to allow them to take steps to reduce risk to their personal data.

Consent gathering

We do not need to get consent from allotment tenants as communication is part of the service we provide to them. Consent forms will sent to new allotment tenants as they join us as tenants.

Privacy notice for allotment holders

Notice will be attached to rental agreement so all residents are given a copy.

Data Controller agreements:

Data controller agreements will be signed by all those who handle data belonging to the PC.

Data Protection Impact Assessments:

A data protection impact assessment will be undertaken before we begin new projects to ensure that we consider any risks to data.