

Sutton-on-Trent Parish Council

Data Protection and Privacy Policy

Sutton-on-Trent Parish Council (the 'Council') recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address. This Data Protection Policy aims to set out what data is collected, where data is collected from, how the Council handles that data and your rights in relation to the data.

As a local authority, the Council is registered with the Information Commissioners Office and has a number of procedures in place to ensure it complies with current legislation regarding the handling of personal data.

General Data Protection Regulations (GDPR)

The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper.

When dealing with personal data, the Council staff and members must ensure that:

- Data is processed fairly, lawfully and in a transparent manner. This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.
- Data is processed for specified purposes only. This means that data is collected for specific, explicit and legitimate purposes only.
- Data is relevant to what it is needed for. Data will be monitored so that too much or too little is not kept; only data that is needed should be held.
- Data is accurate and kept up to date and is not kept longer than it is needed. Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.
- Data is processed in accordance with the rights of individuals. Individuals must be informed, upon request, of all the personal information held about them.
- Data is kept securely. There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

What data is collected

In the course of transacting its business, the Council may collect the following data

- Names, titles and contact details such as telephone numbers, addresses and email addresses
- Where it is relevant to the services provided by the Council, or where you provide it, we may process demographic information such as gender, age, marital status, nationality, family composition, and dependants.
- Website data is classified as activity information and may include information from synching with other software or services, interaction with and access to social media profiles, demographic information. Information collected automatically from the use of the website may include device information, log information including IP address, browser type. Information from cookies may include remembering settings.

Use of personal data

Personal data may be used for some or all of the following purposes

- To deliver public services and to confirm identity to provide some services
- To contact an individual by post, email, telephone or using social media, e.g. Facebook
- To help the Council to build up a picture of how it is performing, to seek views, opinions or comments from residents

- To enable the Council to meet all legal and statutory obligations and powers including any delegated functions

Storing and accessing data

The Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.

The Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely and are not available for public access. All data stored on the Council computer is password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of the Councils document retention policy, it will be shredded or securely deleted from the computer.

The Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy or email). If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period the Council tend to process it for
- Anyone who has access to the personal data

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, the Council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.

Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.

Please see "Subject Access Request Procedure" for more details.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas].

Confidentiality

The Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Changes to this policy

This Data Protection and Privacy Policy is reviewed regularly and was last updated in November 2018.