General Data Protection Regulation Policy draft March 2026

Purpose of the policy and background to the General Data Protection Regulation

This policy explains to Councillors, staff and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government has confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.

This policy explains the duties and responsibilities of the Council and it identifies the means by which the Council will meet its obligations.

Identifying the roles and minimising risk

GDPR requires that everyone within the Council must understand the implications of GDPR and that roles and duties must be assigned, and the Council have a duty to undertake any information audit and to manage the information collected by the Council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.

GDPR requires continued care by everyone within the Council, Councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the Council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also having to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the Council (both financially and reputationally) and one which must be included in the Risk Management Policy of the Council. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the Council undertaking training in data protection awareness.

Data breaches

Personal data breaches should be reported to the Town Clerk for investigation who will conduct this with the support of the Council. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Town Clerk will also have to notify those concerned directly.

1 Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the GDPR) and other local legislation relating to personal data and rights such as the Human Rights Act.

2 Who are the Data Controllers?

• Southwold Town Council (the Town Council)

3 What personal data is collected?

• Names, titles, and aliases, photographs;

• Contact details such as telephone numbers, addresses, and email addresses;

• Where they are relevant to the services provided by the Town Council, or where you provide them to us, we may process demographic information such as gender, age, marital status, nationality, education/work histories, academic/professional

qualifications, hobbies, family composition, and dependents;

• Where you pay for activities such as hire of a stall or attendance at Fair or Civic Dinners, financial identifiers such as bank account numbers, payment / transaction identifiers, policy numbers, and claim numbers;

• The data we process may include sensitive personal data or other special categories of data such as racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sex life or sexual orientation].

• **Demographic information**

4 The Town Council will comply with data protection law. This says that the personal data we hold about you must be:

• Used lawfully, fairly and in a transparent way.

• Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

• Relevant to the purposes we have told you about and limited only to those purposes.

• Accurate and kept up to date.

• Kept only as long as necessary for the purposes we have told you about.

• Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

• To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other services;

• To confirm your identity to provide some services;

• To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);

• To help us build up a picture of how we are performing;

• To prevent and detect fraud and corruption in the use of public funds and where necessary for law enforcement functions;

• To enable us to meet all legal and statutory obligations and power including any delegated functions;

• To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;

• To promote the interests of the council;

• To maintain our own accounts and records;

•

To seek your views, opinions or comments;

• To notify you of changes to our facilities, services, events, staff and Councillors ;

• To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;

• To process relevant financial transactions including grants and payments for goods and services supplied to the council;

• To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The Town Council is a public authority and has certain powers and duties. Most of

your personal data is processed for compliance with a legal obligation which includes the discharge of the Town Council's statutory functions and powers.

Sometime when exercising these powers or duties it is necessary to process personal data of residents or people using the Town Council's services. We will always take into account your interests and rights. This Privacy Policy sets out your rights and the Town Council's obligations to you in detail.

We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

The Town Council will implement appropriate security measures to protect your personal data. This section of the Privacy Policy provides information about the third parties with whom the Town Council will share your personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

• Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
• On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The Town Council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:
When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

(i) The right to access personal data we hold on you
At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.
(ii) The right to correct and update the personal data we hold on you
If the data we hold on you is out of date, incomplete or incorrect, you can inform us and

your data will be updated.

(iii) The right to have your personal data erased

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold. When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

(iv) The right to object to processing of your personal data or to restrict it to certain purposes only

You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

(v) The right to data portability

You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request

(vi) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

(vii) The right to lodge a complaint with the Information Commissioner's Office.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

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.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a Privacy Notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this policy

We keep this Privacy Policy under regular review.

Contact Details:

Please contact us if you have any questions about this Privacy Policy or the personal data, we hold about you or to exercise all relevant rights, queries or complaints at:

Town Clerk townclerk@southwoltowncouncil.com