



South Swindon Parish Council

Data Protection & Information Security Policy

South Swindon Parish Council recognises its responsibility to comply with the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR) which came into effect on 28 May 2018. These regulations regulate the use of personal data. This does not have to be sensitive data; it could be as little as a name or address.

The Data Protection Act 2018 and UK GDPR set 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 Data Protection Act and GDPR applies to anyone holding personal information about people, electronically or on paper.

South Swindon Parish Council has a number of procedures in place to ensure that it complies with The Data Protection Act 2018 and UK GDPR when holding personal information.

When dealing with personal data, South Swindon Parish Council staff and Councillors must ensure that:

- Data is processed fairly and lawfully

This means that personal information should only be collected from individuals if staff and Councillors have been open and honest about why they want the personal information.

- Data is processed for specified purposes only.

- Data is relevant to what it is needed for and will be monitored so that neither too much, or too little is not kept; only data that is needed should be held.

- Data is accurate and kept up to date.

Personal data should be accurate, if it is not it should be corrected.

- Data is not kept longer than it is needed

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

Only staff and Councillors can access the data. It cannot be accessed by members of the public.

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

South Swindon Parish Council may hold personal information about individuals such as their addresses and telephone numbers. These will be securely kept and are not available for public access. Once data is not needed any more, is out of date or has served its use it will be shredded or securely deleted from the computer.

The Parish Council is aware that people have the right to access any personal information that is held about them. If a person requests to see any data that is being held about them:

- They must be sent all of the personal information that is being held about them
- There must be an explanation for why it has been stored
- There must be a list of who has seen it
- It must be sent within one month of receipt. Where a request is complex or numerous, the Council may extend the response period by up to a further two months and will inform the requester of the extension and the reasons for it

A reasonable fee, limited to the Council's administrative costs, may only be charged where a subject access request is manifestly unfounded or excessive, or where the requester asks for additional copies of information that has already been provided

Disclosure of personal information

If a member of the Council needs to access information to help carry out their duties, this is acceptable. They are only able to access as much information as necessary and it should only be used for that specific purpose. Before they have access to any sensitive information about a person, they would need consent to do this from the Parish CEO. Data should never be used for political reasons unless the data subjects have consented.

Personal information in public domain

South Swindon Parish Council does publish contact details of personal individuals that operate with local organisations and charities at the Parish Office and on their website. These are all details that are in the public domain and will be checked regularly to ensure they are kept up to date.

Confidentiality

South Swindon Parish Councillors 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.

GDPR

More information about the new GDPR Regulations is contained in the General Data Protection Regulations Policy. This is available to view on the Parish Council's website and a paper copy is available from the Parish Office.

Personal data breaches

A personal data breach is a security incident that results in the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes, for example, sending information to the wrong recipient, losing a council device or paper file, or unauthorised access to systems containing personal data.

All councillors, employees, volunteers and contractors of the Council are responsible for reporting any actual or suspected personal data breach as soon as they become aware of it. Reports must be made without delay to the CEO (or, in their absence, the Deputy CEO) via email.

On being notified of a possible breach, the CEO will promptly assess the incident, take reasonable steps to contain it, and decide whether it is likely to result in a risk to individuals' rights and freedoms. Where appropriate, the CEO will consult the Chair and take advice from relevant external providers such as IT support.

Where the assessment indicates that the breach is likely to result in a risk to individuals' rights and freedoms, the Council will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, in line with UK data protection law.

Where the breach is likely to result in a high risk to individuals, the Council will also inform those affected directly and without undue delay. The notification will describe in clear and plain language what has happened, the type of data concerned, the steps the Council is taking, and any actions individuals can take to protect themselves.

All personal data breaches, whether or not they are reported to the ICO or to affected individuals, will be recorded in the Council's data breach log. The record will include the facts of the incident, its effects, the outcome of the risk assessment, decisions taken, and remedial actions implemented.

Following any personal data breach, the Council will review the incident to identify any lessons learned and, where necessary, will update procedures, provide additional training, or make technical or organisational improvements to reduce the likelihood and impact of similar incidents in future.

Where a breach arises from failure to follow this Policy or related procedures, the matter may be dealt with under the Council's relevant HR procedures or Councillor Code of Conduct, as appropriate.

Policy Review

This Data Protection Policy will be reviewed annually by the Parish Council. Details of the review and/or amendment will be recorded below.

Date	Description	Page Number	Who
May 2024	Issue	All	CEO/JM
May 2025	Annual Review	All	CEO/JM
May 2026	Annual Review	All	GSL/MT