GDPR Risk Assessment

Name of Council: Southwold Town Council **Date: draft for review May 2026**

Area of risk	Risk Identified	Risk Level H/M/L	Management of Risk	Action taken/completed
All personal data	Personal data falls into hands of a third party	H	Identify what personal data your council holds. Examples include the Electoral Roll, Job applications, tenancy agreements), why it holds it and for how long, who it shares with (see separate Assessment of Personal Data held by councils)	Data audit undertaken by staff. Remains active - ongoing work
		H	Identify how you store personal data. Examples include paper files, databases, electronic files, laptops and portable devices such as memory sticks or portable hard drives.	New filing cabinet keys purchased. Portable hard drive retained in safe. Sort through filing cabinets and destroy confidential waste no longer needed – ongoing basis. Remove emails older than 6 months/1 year if no longer required. Ongoing basis.
	Publishing of personal data in the minutes and other council documents	L	Avoid including any personal information in the minutes or other council documents which are in the public domain. Instead of naming a person, say 'a resident/member of the public unless necessary.	No details written in current format. Historical minutes do display occasionally.
Sharing of data	Personal data falls into hands of a third party	L	Does your council share personal data with any other organisations, for example other local authorities? If yes, you may need to set up a written agreement with the organisation to ensure that they protect the data once passed to them	Occasional share with District and County Councils and will request consent forms going forward asrequired. Confirmed both authorities have procedures in place.
Hard copy data	Hard copy data falls into hands of a third party	L	Decide how much of the personal data held is necessary. Destroy personal data which is no longer needed in line with the Retention of Documents policy	Filing cabinets sorted & destroyed confidential waste no longer needed.
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Clerk's own office, not shared and filing room not shared. Keys for filing cabinet replaced.
		L	If using a shared office operate a clear desk policy when not at desk at the end of the day Cash handling is avoided, but where necessary appropriate controls are in place	Clear desk policy implemented. Cash collected from markets/toilets and retained in safe until bank. Insurance limit adhered to.
Electronic	Theft or loss of a	M	Ensure that all devices are password protected	Ensure passwords are

data	laptop, memory stick or hard drive containing personal data			adequate and reset regularly. Ongoing.
		M	Make all councillors aware of the risk of theft or loss of devices and the need to take sensible measures to protect them from loss or theft	Obtain signed confirmation of "checklist" from all members.
			Carry out regular back-ups of council data	Data backed on external hard drives and kept in safe. Sept 2021 converted to Microsoft 365 administered by I Cloudy.
		L	Ensure safe disposal of IT equipment and printers at the end of their life	Clerk to ensure safe disposal after cleaning system.
		L	Ensure all new IT equipment has all security measures installed before use	Use reputable supplier.I Cloudy supported set up of new equipment Sept 2021 – PC x 2 and laptops.
Email security	Unauthorised access to council emails	L	Ensure that email accounts are password protected and that the passwords are not shared or displayed publically	Safe passwords currently used and only know by owner.
		L	Set up separate parish council email addresses for employees and councillors (recommended)	In place.
		L	Use blind copy (bcc) to send group emails to people outside the council	In place.
		M	Use encryption for emails that contain personal information	In place – and ongoing research to ensure using best system.
		L	Use cut and paste into a new email to remove the IP address from the header	In place.
		L	Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed.	In place.
		H	Delete emails from members of public when query has been dealt with and there is no need to keep it	As per best practice. Consider when does the need pass.
General internet security	Unauthorised access to council computers and files	M	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically	Obtain signed confirmation of "checklist" from all members recommending this action.
		H	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	Obtain signed confirmation of "checklist" from all members.
		M	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Obtain signed confirmation of "checklist" from all members.
		H	Password protect personal and sensitive information folders and databases.	In place - with ongoing

			Ensure that shared drives do not provide unauthorised access to HR and other records containing personal information	research to ensure best system being used.
Website security	Personal information or photographs of individuals published on the website	L	Ensure that you have the written consent of the individual including parental consent if the subject is 17 or under) Ensure you have a Vetting and Barring Policy	Implemented. Only use photographs with permission. Photographs only from accredited sources.
Disposal of computers and printers	Data falls into the hands of a third party	L	Wipe the hard drives from computers, laptops and printers or destroy them before disposing of the device	Noted.
Financial Risks	Financial loss following a data breach as a result of prosecution or fines	L	Ensure that the council has liability cover which specifically covers prosecutions resulting from a data breach and put aside sufficient funds (up to 4% of income) should the council be fined for a data breach Cyber Insurance cover	Noted. Implemented.
	Budget for GDPR and Data Protection	H	Ensure the Council has sufficient funds to meet the requirements of the new regulations both for equipment and data security and add to budget headings for the future	Use of Reserves.
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it	M	Ensure that all staff and councillors have received adequate training and are aware of the risks	Obtain signed confirmation of "checklist" from all members.
	Filming and recording at meetings	L	If a meeting is closed to discuss confidential information (for example salaries, or disciplinary matters), ensure that no phones or recording devices have been left in a room by a member of the public	Noted.

Reviewed on: 26th May 2026 Signed: _____