GDPR Risk Assessment

Name of Council: Warsop Parish Council
Date of Assessment/Review: 9th January 2026
Approval:

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	L	See the Parish Council's **GDPR Policy** for details of what, why, how and for how long data is stored and who it is shared with.	Regularly review to comply with legislation
			Identify how we store personal data. Examples include paper files, databases, electronic files, laptops and portable devices such as memory sticks or portable hard drives.	Ensure data is stored responsibly and securely
	Publishing of personal data in the minutes and other council documents	L	Councillors and staff instructed to avoid including any personal information in the minutes or other council documents which are in the public domain unless strictly necessary. Personal names to be replaced with 'resident/member of the public' when possible.	All documents checked by a second person, where possible before publication
Sharing of data	Personal data falls into hands of a third party	L	The Council does not share personal data with any other person or organisation.	None required.
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 GDPR policy.	
			Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	If personal data is lost or stolen, report to the Clerk
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	L	Ensure that all devices are password protected.	
			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.	If personal data is lost or stolen, report to the Clerk
			Carry out regular back-ups of council data	

			Ensure all new IT equipment has all security measures installed before use	
Email security	Unauthorised access to council emails. Email addresses shared with third parties. Security of email may differ on different devices.	L	Ensure that email accounts are password protected and that the passwords are not shared or displayed publicly.	
		M	Do not share passwords with others. All passwords should be personal, and changed after any resets.	
			Set up separate parish council email addresses for employees and councillors	
		L	Use blind copy (bcc) to send group emails to people outside the council	
			Use encryption for emails that contain personal information	
			Use cut and paste into a new email to remove the IP address from the header	
			Do not forward on emails from members of the public. If necessary, copy and paste information into a new email with personal information removed.	
			Delete emails from members of public when query has been dealt with and there is no need to keep it	
General internet security	Unauthorised access to council computers and files	L	Ensure that all computers and mobile devices are password protected and that the passwords are not shared or displayed publicly	
			Ensure that all computers and mobile devices have up-to-date anti-virus software, firewalls and file encryption is installed.	
			Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	
			Password protect personal and sensitive information folders and databases.	
Website security	Personal information or photographs of	L	Ensure that you have the written consent of the individual before posting photographs or contact information.	

	individuals published on the website			
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	
Financial Risks	Financial loss following a data breach as a result of prosecution or fines		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.	
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.	Ask Councillors to review and sign the GDPR checklist
	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.	Agenda will highlight a closed session or a resolution will be made at the beginning of the meeting.