

GDPR Risk Assessment

Swimbridge Parish Council

Date: 7th January 2024

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 Assessment of Personal Data Held by the Parish Council for details of what, why, how and for how long data is stored and who it is shared with.	
			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.	
	Publishing of personal data in the minutes and other council documents		Councillors and staff instructed to avoid including any personal information in the minutes or other council documents which are in the public domain unless absolutely necessary. Personal names to be replaced with 'resident/member of the public' when possible.	All documents checked by a second Councillor before publication in the public domain.
Sharing of data	Personal data falls into hands of a third party		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		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.	
			Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data		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.	
			Carry out regular back-ups of council data	
			Ensure safe disposal of IT equipment and printers at the end of their life	
			Ensure all new IT equipment has all security measures installed before use	

Email security	Unauthorised access to council emails		Ensure that email accounts are password protected and that the passwords are not shared or displayed publicly	
			Set up separate parish council email addresses for employees and councillors (recommended)	
			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		Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publicly	
			Ensure that all computers (including councillors) 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. Ensure that shared drives do not provide unauthorised access to HR and other records containing personal information	
Website security	Personal information or photographs of individuals published on the website		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	
Disposal of computers and printers	Data falls into the hands of a third party		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	

	Budget for GDPR and Data Protection		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	
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it		Ensure that all staff and councillors have received adequate training and are aware of the risks.	
	Filming and recording at meetings		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.	

Reviewed on: _____ **Signed:** _____ **(Chairman)**