Local Council Public Advisory Service

GDPR Risk Assessment

Name of Council: Astley Village Parish Council **Date: September 2021**

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.	
		L	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 Parish Council documents	L	Parish Councillors and Parish Clerk instructed to avoid including any personal information in the minutes or other Parish Council documents which are in the public domain unless absolutely necessary. Personal names to be replaced with 'resident/member of the public' when possible.	
Sharing of data	Personal data falls into hands of a third party	L	The Parish Council does not share personal data with any other person or organisation.	
Hard copy data	A hard copy of 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 Document Retention Policy.	
		L	Ensure that sensitive personal data is stored securely in a locked cabinet when not in use	

Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	L	Ensure that all devices are password protected.	
		L	Make all Parish 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.	
		L	Carry out regular back-ups of Parish Council data	
		L	Ensure safe disposal of IT equipment and printers at the end of their life	
		L	Ensure all new IT equipment has all security measures installed before use	
Email security	Unauthorised access to Parish Council emails	L	Ensure that email accounts are password protected and that the passwords are not shared or displayed publically	
		L	Parish Council email addresses provided for Parish Clerk and Parish Councillors and Parish Councillors are recommended not to use personal email addresses for Parish Council business.	
		L	Use blind copy (bcc) to send group emails to people outside the Parish Council	
		L	For devices set up by our web/email host, encryption for emails will be set up.	
		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.	
General internet security	Unauthorised access to computers and files where Parish Council information is accessed/stored	L	All electronic devices used to access emails/Parish Council information (including Parish Councillors) should be password protected and that the passwords are not shared or displayed publicly	
		L	Ensure that all computers (including Parish Councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	
		L	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	
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 18 or under)	
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	L	Ensure that the Parish 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 Parish Council be fined for a data breach	
	Budget for GDPR and Data Protection	L	Ensure the Parish 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	L	Ensure that the Parish Clerk and Parish Councillors have received adequate training and are aware of the risks.	
	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.	

Reviewed on: _____ Signed: _____ (Chairman)