

# Beckley Parish Council

## Risk Assessment

Adopted by the Council 9 May 2018

Area of risk	Risk Identified	Risk Level H/M/L	Management of Risk	Action taken/completed
<b>All personal data</b>	Personal data falls into hands of a third party		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)	
			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.	
	Publishing of personal data in the minutes and other council documents		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.	
<b>Sharing of data</b>	Personal data falls into hands of a third party		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	
<b>Hard copy data</b>	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	
			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	
<b>Electronic data</b>	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	
<b>Email security</b>	Unauthorised access to council emails		Ensure that email accounts are password protected and that the passwords are not shared or displayed publically	
			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	
<b>General internet security</b>	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 publically	
			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	
<b>Website security</b>	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	
<b>Disposal of computers and printers</b>	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	
<b>Financial Risks</b>	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	
<b>General risks</b>	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	