Parish Office, Sports Pavilion, Hundred Acre Way, Red Lodge, Suffolk, IP28 8FQ

GDPR Risk Assessment

Name of Council: Red Lodge Parish Council **Date: 16/05/2023**

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	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)	Personal data stored in a restricted secure cabinet
		L	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.	Personal data stored in paper files
	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.	Personal data is not published, a generic term is used
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	N/A
Hard copy data	Hard copy data falls into hands of a third party	M	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	Personal data is shredded
		M	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Personnel information is stored in a secure cabinet
		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	Desks are kept clear and locked. Petty cash is handled

Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	L	Ensure that all devices are password protected	All devices are password protected
		L	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	A signed agreement with councillors to adhere to good practices
		L	Carry out regular back-ups of council data	Data backed up regularly
		L	Ensure safe disposal of IT equipment and printers at the end of their life	IT equipment will be destroyed
			Ensure all new IT equipment has all security measures installed before use	IT support ensures security is in place
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	Emails are password protected
		L	Set up separate parish council email addresses for employees and councillors (recommended)	All emails are separated
		L	Use blind copy (bcc) to send group emails to people outside the council	N/A
		L	Use encryption for emails that contain personal information	N/A
		M	Use cut and paste into a new email to remove the IP address from the header	Cut and paste is used
		M	Do not forward on emails from members of the public. If necessary, copy and paste information into a new email with personal information removed.	Information is copied and pasted,personal information is removed.
		M	Delete emails from members of public when query has been dealt with and there is no need to keep it	Old emails are deleted once dealt with
General internet security	Unauthorised access to council computers and files	L	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically	Passwords are protected and kept discrete
		L	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	IT support installed appropriate up to date protection
		L	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Operating systems reviewed regularly
		L	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	Shared drives do not contain personal data
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	N/A

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	IT support wipe the devices accordingly
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	Liability cover is in place
	Budget for GDPR and Data Protection	L	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	Budget has been allowed for GDPR
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it	L	Ensure that all staff and councillors have received adequate training and are aware of the risks	Staff are briefed with GDPR bulletins and information
	Filming and recording at meetings	M	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	Any recording devices are switched off during a confidential discussion

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