KENWYN PARISH COUNCIL
GDPR Risk Assessment

Name of Council: **Date:**

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)	1. No longer hold the Electoral Roll 2.Job applications are destroyed once staff are employed, at application stage each applicant is asked for permission to hold their details until the appointment is made. 3.Council does not hold any tenancy agreements
		M	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.	1. Paper files have been pruned and all unnecessary documents shredded. 2. Databases, electronic files, laptops, portable devices, external hard drives, storage drives are all password protected. External storage devices are stored in the office safe. Virus protection is installed and firewalls are turned on at all times. Memory sticks are not used as the data cannot be password protected.
	Publishing of personal data in the minutes and other council documents	M	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.	To date the person's name would be in the minutes. From 1st May onwards no names will feature in the minutes unless absolutely necessary to do so.

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	The parish council does not share data with other organisations.
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 Retention of Documents policy	No longer held
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Any sensitive data which is now kept to a minimum is locked in safe
		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	1. The office is not shared. 2.Cash handling is minimal and any cash is banked the same day.
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. Memory sticks are not used. All external hard drives are stored in the safe.
		M	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	Councillors have been made aware of these risks and have been asked to complete and return the General Data Protection Awareness Checklist for Councillors
		L	Carry out regular back-ups of council data	1. PC is regularly backed up and external storage device stored in the safe.
		L	Ensure safe disposal of IT equipment and printers at the end of their life	Computers/laptops are stripped down and the hard drives removed and destroyed before disposal
		L	Ensure all new IT equipment has all security measures installed before use	This is complied with on every occasion
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	Councillors have now been provided with dedicated email addresses, passwords are not shared or displayed anywhere publically
		L	Set up separate parish council email addresses for employees and councillors (recommended)	Completed in February 2018

		L	Use blind copy (bcc) to send group emails to people outside the council	This method has been employed by the Clerk for several years
		M	Use encryption for emails that contain personal information	Unable to do so as IT requirements between Office and Councillors not available.
		M	Use cut and paste into a new email to remove the IP address from the header	Councillors instructed to employ this method when communicating externally and Clerk now using this system
		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.	Councillors instructed to employ this method when communicating externally and Clerk has been using this system for several years
		M	Delete emails from members of public when query has been dealt with and there is no need to keep it	Clerk already does this. Councillors asked to do the same
General internet security	Unauthorised access to council computers and files	M	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically	All council computers and laptops are password protected. Councillors asked to do the same to their devices and sign the form confirming this
		M	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	All council computers and laptops are protected by up-to-date anti-virus protection software and firewalls. Councillors asked to do the same to their devices and sign the form confirming this. Encryption not possible
		L	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Already in place
		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	Already in place
Website security	Personal information or photographs of individuals published on the	M	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	Consent requests have been sent to all contacts, logs have been created to record the consents and a hard copy of the consents is kept in the

	website			office, Policy to be adopted at the next meeting
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	Already use this system, hard drives are always removed and destroyed before devices, laptops or computers are disposed of. Councillors asked to do the same.
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	Insurance cover in place as of 25th May 2018 and £5300 set aside from reserves for any potential data breach fines (4% of all income with the exception of the Community Benefit Fund Payments from Solar Farms where council acts as administrator only)
	Budget for GDPR and Data Protection	M	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	This is unexpected expenditure not known about or budgeted for 2018-19. However the council has healthy reserves and can manage this risk this year. In future years a budget will be held for this and it will be closely monitored
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	LCPAS has been employed to assist the council, Clerk is becoming well versed in the regulations. Councillors should attend training courses and this can be funded by the council
	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	Clerk asks at every meeting if anyone is recording. Clerk and Council to ensure all recording devices have been removed from the meeting where the council is in confidential, closed session. Clerk has marked out a clear public gallery area and recording policy is on display at all times.

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