GDPR Risk Assessment

Name of Council: Lane End Parish Council **Date: 9th April 2018**

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		Electoral Roll Allotment Tenancy Agreements Letters from residents Emails from residents Contact details for Parish/District/ County Councillors Contact details for Parish organisations Parish Plan Clerks employment details Playing Field manager employment details Complaints Grant / donation applications Planning applications Contractor details Third parties – County & District Councils, other Parish / Town Councils Email addresses IP address Purchase History Downloads PAYE Subscription services Information relating to children Website Clarion Agenda & Minutes Identify what personal data is held. (see separate Assessment of Personal Data)	Stored on clerk's laptop which is in her home. Laptop is password protected as are the council internet accounts. The laptop has a firewall and anti-virus software and the laptop is updated regularly. Clerk no longer forwards on personal emails but uses saves them and sends them as an attachment or copies and pastes information from the email. See Assessment of personal data.
			Identify how to store personal data.	Paper Files, Laptop, memory Device.
	Publishing of personal data in the minutes and other council documents		No personal information are published in the minutes or other council documents which are in the public domain.	State resident or parishioner.

Sharing of data	Personal data falls into hands of a third party		No personal data to be shared. If data is shared Council must set up a written agreement with the organisation to ensure that they protect the data once passed to them	Any personal data can only be sent via The Clerk with consent.
Hard copy data	Hard copy data falls into hands of a third party		Destroy personal data which is no longer needed in line with the Retention of Documents policy	Clerk working through this.
			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	
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data		Laptop is password protected	Complete.
			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 made aware at the PC meeting on 9th April 2018.
			Carry out regular back-ups of council data	Daily - Clerk
			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	Complete
Email security	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)	Clerk – complete Councillors – to be set up
			Use blind copy (bcc) to send group emails to people outside the council	Daily
			Use encryption for emails that contain personal information	Daily
			Use cut and paste into a new email to remove the IP address from the header	Daily
			Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed.	Daily
			Delete emails from members of public when query has been dealt with and there is no need to keep it	Daily
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 publically	Clerk – complete Councillors – to action
			Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	Clerk – complete Councillors – to action
			Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Clerk – complete Councillors – to action
			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)	
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	None
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 ensure that no phones or recording devices have been left in a room by a member of the public	

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