General Data Protection Risk Assessment

Name of Council: Kelsale-cum-Carlton Parish Council **Date: 25/05/2018**

Area of risk	What are the Risk(s)?	How are the risk(s) already being managed?	Further Action Needed	Responsible Person	Date Action To be Completed by	Date Completed
All personal data	Personal data falls into hands of a third party	Information Asset Register in place which identifies all data currently being held by the Parish Council and where any data is shared with other agencies. Data Retention Policy in place.	Annual review of Asset Register. Annual review of Data Retention Policy Process to be developed to ensure that Data Retention Policy is being effective.	The Clerk	July 2019	
		Appendix included in Asset Register which lists how data is stored including both hard copy data and electronic data.	Update Appendix if any changes are made, for example a new piece of hardware or alternative methods of storage introduced.	The Clerk	Ongoing updates	
	Publishing of personal data in the minutes and other council documents	Protocol in place to protect the identities of the public by having them remain anonymous when reported in the minutes. Protocol in place to redact names of the public when documents are uploaded onto the website. If a person needs to be identified, a consent form is available which **must** be completed before any minutes or documents can be published.	Protocols to be formally written up as part of GDPR compliance. This will form part of the GDPR Policy.	The Clerk	End July 2018	
Sharing of data	Personal data falls into hands of a third party	No work has been done regarding this to date.	Work to be completed to identify which organisations the Parish Council shares data with. To be inserted into the Information Asset Register. Written agreements to be produced for any such organisations.	The Clerk	End of August 2018	

Area of risk	What are the Risk(s)?	How are the risk(s) already being managed?	Further Action Needed	Responsible Person	Date Action To be Completed by	Date Completed
Hard copy data	Hard copy data falls into hands of a third party	Data Retention Policy in place. Data due to be destroyed is shredded and disposed of by a licensed company.	Annual review of Data Retention Policy.	The Clerk	July 2019	
		Sensitive data is kept in a fire proof filing cabinet.	Annual check of filing cabinet to ensure it is fit for purpose,	The Clerk	July 2019	
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	Email, Internet & Social Media Policy in place which states that anyone conducting Parish Council business must have a working password on their device.	Annual review of Email, Internet & Social Media Policy.	The Clerk	July 2019	
		Regular back-ups are taken and saved onto a RAID 1 hard drive.		The Clerk	September 2018	
		Protocol in place to ensure compliance to The Waste Electric and Electronic Equipment (WEEE) Regulations 2013.	Protocol to be formally written up and will form part of the Health and Safety Risk Assessments. This will also include the wiping of any hard drives or other devices prior to disposal.	The Clerk	December 2018	
		Nothing in place ensuring that any new IT equipment has adequate security and encryption software installed before use.	IT Data Protection Policy to be written to include protocols regarding new IT hardware.	The Clerk	December 2018	
Email security	Unauthorised access to council emails	The Clerk and each member of the Council has been issued with a Council email address. Protocols regarding this are contained in the Email, Internet and Social Media Policy.	The Clerk and Councillors to be reminded to change their passwords regularly to increase security.	The Clerk	Every 12 months	
		A protocol in place to use blind copy (bcc) when sending group emails to people outside the council. The protocol is contained in the Email, Internet & Social Media Policy.	No further action required.			

		Encryption software is available on the Parish Council laptop.	Councillors to be requested to install encryption software if they are going to be sending confidential or personal data via email.	The Clerk	End of July 2018	
		A protocol is in place ensuring that emails received by members of the public are not forwarded. This is to ensure that their personal information is removed from view of new recipients. Instead the content of the email should be copied and pasted into a new email with the relevant information only. This protocol is contained in the Email, Internet & Social Media Policy.	No further action needed.			
		A protocol is in place to delete emails from members of the public once a query has been dealt with to protect their personal information. This protocol is contained in the Email, Internet & Social Media Policy.	No further action needed.			
Website security	Personal information or photographs of individuals published on the website	Formal Website policy to be developed as soon as possible.	This policy will need to include: • Written consent of any individuals whose photographs or copy have been used on the website. • Parental consent if the subjects are under the age of 17.	The Clerk/Cllr Galloway	August 2018	
Financial Risks	Financial loss following a data breach as a result of prosecution or fines	No provision known for this at present.	Need to ensure that the Council has liability cover which specifically covers prosecutions resulting from a data breach and put aside sufficient funds (up to	The Clerk	Work in Progress	

			4% of income) should the Council be fined for a data breach.			
	Budget for GDPR and Data Protection	Authorisation for sufficient funds has been given by the Parish Council to ensure that it complies with the new regulations for both new equipment and data security.	GDPR will need to be added as a budget heading in the future and allocated sufficient funding to ensure continued compliance with the new regulations.	The Clerk	October 2018	
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it	No work has been undertaken on this to date.	Research needed to find out best practice in how to manage this aspect of the regulations.	The Clerk	Work in Progress	
	Filming and recording at meetings	No work has been undertaken on this to date.	Protocol to be put in place to ensure that if a meeting is closed to discuss confidential information (for example salaries, or disciplinary matters) no phones or recording devices have been left in a room by a member of the public.	The Clerk	August 2018	

Signed: _____ (Chairman) Date _____

Review Date: May 2019