GDPR Risk Assessment

Name of Council: Chelmondiston Parish Council **Date: 20/07/2018**

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	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)	**Electoral Roll, Clerk's personnel information, telephone numbers, planning applications and decisions, letters from the public, dinghy park information, grant and funding information, cv's, parish councillor's resignations, parish councillor's applications,**
		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.	**Laptop double password protected. Lockable drawers in Clerk's office for hard copies. Historic information contained in a container that is locked.**
	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.	**No personal information is included.**
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	**No information shared.**
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	**Hard data is destroyed re the retention policy. All personal data is locked and secure. The container is also locked and secure.**

		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	**All hard copy and sensitive information as above**
		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	**All information is locked unless needed then filed away.**
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	L	Ensure that all devices are password protected	**Laptop is double password protected.**
		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	**All councillors have signed the councillor's awareness checklist and a reminder recorded in 07/08/2018**
		L	Carry out regular back-ups of council data	**Completed regularly**
		L	Ensure safe disposal of IT equipment and printers at the end of their life	**Retention Policy highlights the procedure**
		L	Ensure all new IT equipment has all security measures installed before use	**Completed**
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	**Double password protected**
		H	Set up separate parish council email addresses for employees and councillors (recommended)	**Parish Clerk separate email address. Councillors awareness checklist has been signed by all Cllrs and a reminder recorded 07/08/2018**
		L	Use blind copy (bcc) to send group emails to people outside the council	**Always**
		L	Use encryption for emails that contain personal information	**Not Used**
		L	Use cut and paste into a new email to remove the IP address from the header	**Used if the sender does not give consent**
		L	Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed.	**Used if the sender does not give consent**
		L	Delete emails from members of public when query has been dealt with and there is no need to keep it	**Emails deleted once query has been dealt with**
General internet security	Unauthorised access to council computers and files	H	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically	**Clerk's protected. Cllrs all signed the awareness checklist. A reminder recorded 07/ 08 /2018**
		H	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	**Clerk's protected. Cllrs signed the awareness checklist and recorded as a reminder 07/08/2018**

		M	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	**Councillors and Clerk to ensure that this happens**
		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	**When sensitive information a separate folder will be password protected.**
Website security	Personal information or photographs of individuals published on the website	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** **Chelmondiston Parish Council has The Criminal Bureau Disclosure and Barring Service: The Code of Practice. Adopted 03/02/2009. Reviewed 07/04/2015. Reviewed 04/07/2017.**	**N/A at the moment. However, process in place.** **The Criminal Bureau Disclosure and Barring service: The Code of Practice to be reviewed 02/10/2018**
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	**Chelmondiston Parish Council to conform to the Document and Electronic Data Retention Policy**
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	**Chelmondiston Parish Council has liability cover.** **4% of income to be ringfenced if the council is fined for a data breach to agenda for discussion in the Finance Advisory Committee and then to approve in Novembers 2018Parish Council Meeting.**
	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	**To be discussed in the Finance Advisory Committee and then approved in Novembers 2018 Parish Council Meeting.**
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	**Cllrs awareness checklist completed. Reminder 07/08/2018**
	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	**Actioned**

Reviewed on: 7/8/18 **Signed:** _____ **(Chairman)**

Highlighted in Red = Discussion at 07/08/2018 Meeting before agreement of Chairman signs.

Highlighted in Blue = Discussion of completion of dates (October and November 2018) of tasks to complete before agreement of Chairman signs.