Local Council Public Advisory Service

GDPR Risk Assessment

Name of Council: Marlesford Parish Council

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)	Discussion with clerk about what data we hold – mostly just names, addresses and phone numbers
		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.	Councillors all reminded of the need to safeguard data
	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.	Clerk aware and will be monitored by the DPO
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	Not applicable
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	Clerk and councillors aware
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Data held in clerk's private and secure house
		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	Not applicable
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal	L	Ensure that all devices are password protected	Clerk's PC is password protected

	data			
			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	Checklist circulated to all councillors
			Carry out regular back-ups of council data	Clerk is so doing
			Ensure safe disposal of IT equipment and printers at the end of their life	DPO will organise when required
			Ensure all new IT equipment has all security measures installed before use	DPO will organise when required
Email security	Unauthorised access to council emails		Ensure that email accounts are password protected and that the passwords are not shared or displayed publically	Clerk's email is password protected
			Set up separate parish council email addresses for employees and councillors (recommended)	Only applies to the RFO who is not on the parish councillor's list
			Use blind copy (bcc) to send group emails to people outside the council	Noted
			Use encryption for emails that contain personal information	Will be deleted when not required
			Use cut and paste into a new email to remove the IP address from the header	Noted
			Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed.	Noted
			Delete emails from members of public when query has been dealt with and there is no need to keep it	All aware
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	Councillors advised. NB all councillors work from their private homes
			Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	Councillors advised
			Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Councillors advised
			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	Not Applicable
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	DPO will organise when required
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	Council insurance covers liability for costs associated with a data breach but insurers do not provide cover against legal penalties.
	Budget for GDPR		Ensure the Council has sufficient funds to meet the requirements of the new	Noted

	and Data Protection		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	Councillors have received a briefing note and are updated at PC meetings
	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	DPO will undertake

Reviewed on: 24th March 2021 **Signed:** *Melanie Thurston - Clerk* *pp* **(Chairman)**