Kimberley Town Council

GDPR Risk Assessment

Adopted by Full Council on 30th March 2023 TC/23/454
Reviewed by Full Council 27th March 2025TC/25/213

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	See **Assessment of Personal Data Held by the Parish Council** for details of what, why, how and for how long data is stored and who it is shared with.	Data Protection Awareness Policy/Checklist
		L	Identify how we store personal data. Examples include paper files, databases, electronic files, laptops and portable devices such as memory sticks or portable hard drives.	Data Protection Awareness Policy/Checklist
	Publishing of personal data in the minutes and other council documents	L	Councillors and staff instructed to avoid including any personal information in the minutes or other council documents which are in the public domain unless absolutely necessary. Personal names to be replaced with 'resident/member of the public' when possible.	Clerk to follow process, Members to check for personal data in draft minutes.
Sharing of data	Personal data falls into hands of a third party	M	The Council does not share personal data with any other person or organisation.	Covered by the Privacy Policy and KTC General Data Protection Awareness Checklist for Councillors to be signed buy all Councillors.
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.	Ongoing.
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Laptops are locked in office outside working hours.

Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	M	Ensure that all devices are password protected, passwords changed monthly.	Password for laptops and email.
		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.	Covered in checklist for new members.
		L	Carry out regular back-ups of council data	Ongoing.
		L	Ensure safe disposal of IT equipment and printers at the end of their life	Ongoing.
		L	Ensure all new IT equipment has virus/password/cloud back in place before use.	Ongoing.
Email security	Unauthorised access to Council emails	L	Ensure that email accounts are password protected and that the passwords are not shared or displayed publicly.	Ongoing.
		L	Set up separate Town Council email addresses for employees and Councillors (recommended)	In progress.
		L	Use blind copy (bcc) to send group emails to people outside the Council.	Ongoing.
		L	Use encryption for emails that contain personal information.	Check file encryption available.
		L	Use cut and paste into a new email to remove the IP address from the header	Ongoing.
		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.	Ongoing.
		L	Delete emails from members of public when query has been dealt with and there is no need to keep it	Ongoing.
General internet security	Unauthorised access to Council computers and files	L	Ensure that all computers (including Councillors) are password protected and that the passwords are not shared or displayed publicly	To be implemented.
		L	Ensure that all computers (including Councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	To be implemented.
		M	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	To be implemented.
		M	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	To be implemented.
Website security	Personal information or photographs of individuals published on the website	L	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	Adopted as policy. DBS not essential for members.
	Access Controls	L	Only Clerk and one other person can update the Website Only Clerk and one other person can update KTC's social media pages	Adopted as policy
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. Use Cavendish Systems to carry out data backup and then full deletion	Adopted as 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	To be implemented.
	Budget for GDPR and Data Protection	L	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 implemented.
General risks	Loss of third-party data due to lack of understanding of the risks/need to protect it	L	Ensure that all staff and Councillors have received adequate training and are aware of the risks.	Adopted as policy New Councillors to sign checklist. GDPR policy now implemented.
	Filming and recording at meetings	L	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.	Ongoing.