FRAMLINGHAM TOWN COUNCIL RISK ASSESSMENT AND PROCEDURE RECORD (See Guidance for performing and reviewing Risk Assessments)

GDPR
Reviewed Cllr S Garrett Nov 2021
Approved by Full Council on: 2022/01/06

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	M	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)	List of personal data held with GDPR forms in yellow folder
			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.	All locked in cupboard or filing cabinets
	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.	Council documents go through a stage of drafts and proofing to ensure compliance before publication
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	Only statutory 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	Minimum data is kept and then only for as long as needed. Paper is shredded and Retention of Document Policy Followed
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Locked filing cabinets are used only by staff
		M	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	Care must be taken with documents on desks when public are at window hatch
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	L	Ensure that all devices are password protected	All laptops are password protected
		L	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	Training given to Cllrs
		H	Carry out regular back-ups of council data	Data backed up weekly to hard drives which are not password protected – need to protect the data on the back up drives

		L	Ensure safe disposal of IT equipment and printers at the end of their life	Professional data destroyers to be used
		L	Ensure all new IT equipment has all security measures installed before use	Town Clerk ensures this is done
Email security	Unauthorised access to council emails	H	Ensure that email accounts are password protected and that the passwords are not shared or displayed publicly	completed
		H	Set up separate town council email addresses for employees and councillors (recommended)	Recommended by ICO or make sure Councillors keep separate folder for Council business
		M	Use blind copy (bcc) to send group emails to people outside the council	Staff check cc lists before sending every time
		H	Use encryption for emails that contain personal information	Not in place
		M	Use cut and paste into a new email to remove the IP address from the header	Following training, staff are aware of this need
		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.	This is the procedure that is followed at present
		L	Delete emails from members of public when query has been dealt with and there is no need to keep it. Where there is follow-up correspondence (or follow-up is considered likely), then it is prudent to retain all related email correspondence until the matter is closed to the satisfaction of the Council and the correspondent. In case of doubt, correspondence should be kept for 6 months after the last correspondence on the matter.	This should be done every time the computer is backed up
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 publically	All computers are password protected
		M	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	recommended
		M	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Windows 10 currently used on all laptops.
		H	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	Hard drives need password protecting, need to install axcrypt or similar
Website security	Personal information or photographs of individuals published on the website	M	Ensure that you have the written consent of the any individual under 18 including parental consent Ensure you have a Vetting and Barring Policy	Consent forms available

Disposal of computers and printers	Data falls into the hands of a third party	M	Wipe the hard drives from computers, laptops and printers or destroy them before disposing of the device	Medium risk as this has not been tested under GDPR environment. A data destruction and encryption programme will help
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	GDPR is covered on insurance.
	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	Budget 1138
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	Training on GDPR for all Cllrs and staff 15/03/18 GDPR refresher – Town Clerk 17/02/2020
	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	A visual sweep is made after any public have left at every meeting