BEXHILL-ON-SEA TOWN COUNCIL GDPR Risk Assessment 2021

Date: 1ST September 2021

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)	Data is held on a password protected OneDrive account.
		M	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 has password, portable files are kept in a locked cabinet in the town hall office temporarily.
	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.	Minutes checked by Clerk before publishing.
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 such data is currently held.
Hard copy data	Hard copy data falls into hands of a third party	M	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	Regular reviews of emails and paper files, retention policy to be adopted at October meeting
		M	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	In Town Hall locked cabinet. Clerk retains key.
			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	No paperwork is left on desk in town hall.
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	M	Ensure that all devices are password protected	Laptop is password protected.
		H	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	Councillors reminded of risks of using personal devices for council emails/documents.
		L	Carry out regular back-ups of council data	OneDrive auto backs up to the cloud.
		L	Ensure safe disposal of IT equipment and printers at the end of their life	IT consultant to be sought to assist with destruction of hardware if needed.

		M	Ensure all new IT equipment has all security measures installed before use	Antivirus software installed and password protected.
Email security	Unauthorised access to council emails	M	Ensure that email accounts are password protected and that the passwords are not shared or displayed publically	All users have changed password that only they know. Reminder to all councillors not to store passwords or share with anyone.
		H	Set up separate parish council email addresses for employees and councillors (recommended)	All councillors with the exception of Cllr Thomas are using .gov.uk emails. Council business no longer being sent to Cllr Thomas' private email address.
		H	Use blind copy (bcc) to send group emails to people outside the council	Councillors to be mindful that email addresses of people outside of the council are not shared inadvertently on email through replying or forwarding.
		M	Use encryption for emails that contain personal information	Personal Data files must be password protected.
		M	Use cut and paste into a new email to remove the IP address from the header	Councillors reminded of this process.
		H	Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed.	Councillors reminded of this process.
		H	Delete emails from members of public when query has been dealt with and there is no need to keep it	Councillors reminded of this process.
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	The council does not currently have any PC hardware. Laptop password is confidential.
		L	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	The council does not currently have any PC hardware. Laptop has anti virus software.
		L	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Auto updates are in place on laptop.
		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	One Drive password protected files.
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	The council will adopt a vetting and barring policy and parental consent form at the October meeting.
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	IT consultant to assist with future destructions.
Financial Risks	Financial loss	M	Ensure that the council has liability cover which specifically covers prosecutions	Zurich Insurance Policy,

	following a data breach as a result of prosecution or fines		resulting from a data breach and put aside sufficient funds (up to 4% of income) should the council be fined for a data breach	contingency reserves exist for data breach fines.
	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	Council has IT budget
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it	H	Ensure that all staff and councillors have received adequate training and are aware of the risks	There have been two potential GDPR breaches of councillors forwarding emails outside of the council without permission. This has been reported to the ICO. The council has a policy in place for GDPR to address this.
	Filming and recording at meetings	M	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	Chairman to confirm at each meeting.

Reviewed on: _____ **Signed:** _____ **(Chairman)**