ST BREOCK PARISH COUNCIL RISK ASSESSMENT- GDPR SPECIFIC

This document has been produced to enable St Breock Parish Council to assess the risks that it faces and satisfy itself that it has taken adequate steps to minimise them. In conducting this exercise, the following plan was followed:

- Identify the areas to be reviewed.
- Identify what the risk may be.
- Evaluate the management and control of the risk and record all findings.
- Review assess and revise if required.

Subject	Risk(s) Identified	H/M/L	Management/Control of Risk	Review/Assess/Revise
All personal data	Personal data falls into hands of a third party	H	Identify what personal data St Breock Parish 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)	Carry out Data Audit
	Publishing of personal data in the minutes and other council documents	M	Identify what personal data is stored. Examples include paper files, databases, electronic files, laptops and portable devices such as memory sticks or portable hard drives.	Remove emails over 6 months if no longer required.
Sharing of data	Personal data falls into hands of a third party	L	Does our 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 share with those Councils who have similar procedures in place.
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	Destroy any confidential waste no longer needed

			longer needed in line with the Retention of Documents policy	
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	Existing procedure adequate
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	L	Ensure that all devices are password protected	Existing procedure adequate
		M	Make all councillors aware of the risk of theft or loss of any devices with Council emails on and the need to take sensible measures to protect them from loss or theft	A reminder to all Members by reading this document.
	.	H	Carry out regular back-ups of council data	Need to undertake more often.
		L	Ensure safe disposal of IT equipment and printers at the end of their life	Existing procedure adequate
Email security	Unauthorised access to council emails	L	Ensure that all computers/laptops have up to date anti-virus software and firewalls .	Existing procedure adequate
		M	*Set up separate Parish Council email* addresses for employees and councillors (recommended).	*Re visit as declined in 2018*
		L	Use blind copy (bcc) to send group emails to people outside the council	Existing procedure adequate
		M	Use cut and paste into a new email to remove the IP address from the header	Existing procedure adequate
		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	Existing procedure adequate

		H	Delete emails from members of public when query has been dealt with and there is no need to keep it	Need to consider what to keep?
General internet security	Unauthorised access to council computers and fil	M	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publicly	Existing procedure adequate
		H	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed	Existing procedure adequate
		M	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Existing procedure adequate
		H	Password protect personal and sensitive information folders and databases. Ensure that shared drives do not provide unauthorised access to Council computers and files or, any other records containing personal information	Rarely an issue.
Website security	Personal information or photographs of individuals	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	Rarely an issue. Investigate if policy is needed.
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 Clerk	To date, this has not been required to be undertaken.
Financial Risks	Financial loss following a data breach as a result of prosecution or fines	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	Existing procedure adequate

			Budget	
	Budget for GDPR and Data Protection	H	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	Does this need to be considered?
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	
	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	Rarely an issue.

Review of Risk Assessment due:

Signed: _____ Chairman Signed: _____ Parish Clerk/RFO Date: 10/04/19