General Data Protection Regulations

The new General Data Protection Regulations come into force on 25 May 2018.

The EU's General Data Protection Regulation (GDPR) will apply from 25 May 2018, when it supersedes the UK Data Protection Act 1998. Significant and wide-reaching in scope, the new law brings a 21st century approach to data protection. It expands the rights of individuals to control how their personal information is collected and processed, and places a range of new obligations on organisations to be more accountable for data protection. It will not be affected by Brexit.

GDPR compliance is not just a matter of ticking a few boxes; the Regulation demands that we are able to demonstrate compliance with the data protection principles. This involves taking a risk-based approach to data protection, ensuring appropriate policies and procedures are in place to deal with the transparency, accountability and individuals' rights provisions, as well as building a workplace culture of data privacy and security.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and legally.
- Personal data must only be obtained for specified and legal purposes, and must only be processed in a way that is consistent with the specified purpose.
- Personal data must be adequate, relevant and not excessive for the purpose it is processed for.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose must not be kept longer than is necessary to fulfil that purpose.
- Personal data must be processed in line with the data subject's rights
- Appropriate security measures must be taken to protect against unauthorised or illegal data processing.
- Transferring personal data outside of the European Economic Area is restricted unless the rights and freedom of data subjects are protected.

What do we need to do?

- Review procedures & document this. Establish where data comes in, what data is collected, how it is used and when it is disposed of.
- IT control. Review where data is stored and where necessary obtain any third party agreements. Ensure data is stored with Europe (eg – any cloud storage). The Parish Council website will require an SSL Certificate. (**SSL Certificates** are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.)

- A number of policies and procedures will need to be put in place to make GDPR work. Such as Data protection Policy, IT policy, Email retention policy etc.
- Training – all staff and councillors should have training on this.

Recommendations

Action	Reason	Cost
Internal Audit of data controls	To establish what exactly data comes in to the Parish Council via the Clerk and Councillors	£80.00
Training	So that all Councillors are aware of the regulations and the duties of the Parish Council as Data Controller and the Clerk/Councillors as Data Processors.	£400 *
Obtain an SSL certificate for the Parish Council Website	A SSL Certificate guarantees that sensitive data shared between your server and your users browser, is secure and safe.	From £50 pa
Professional IT Management	To safeguard the Parish Council from any possible issues from website hacks/data theft	From £200 pa
Data Protection Officer	This needs to be an independent professional person. Not the Clerk or a Councillor. It is understood that neither the County Council or District Council are going to provide this service for Parish Councils. A number of options are being put forward but these are all subject to fees.	From £150.00 pa
Use of MS Sharepoint	This gives proper control to the Parish Council – Freedom of Information (FOI) or Data Protection requests are much easier to handle and avoids the issue of Councillors having any data on their own personal computers.	From £450 pa