The Data Protection Policy

Sherfield English Parish Council recognises its responsibility to comply with the Data Protection Act 1998 and the introduction of the General Data Protection Regulations 25 May 2018. The Act regulates the use of personal data "relating to an identified or identifiable natural person". This can be any data by which an individual can be identified for example, this can be as little as a name and address, but it can also include identification numbers, location data, online identifier or other more specific factors such as physical, psychological, genetic, mental, economic, cultural or social identity. In addition, the GDPR specifically prohibit the processing of 'special category data' unless there is a legitimate requirement or the individual has given their explicit consent to the processing. Special category data is defined as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (Article 9 – GDPR).

The Data Protection Act 1998 and subsequent GDPR, set out high standards for the handling and retention of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. These Data Protection requirements apply to organisation holding personal information about people, electronically or on paper. Sherfield English Parish Council has also notified the Information Commissioner's Office (ICO) that it potentially holds personal data about individuals. When dealing with personal data, Sherfield English parish council members must ensure that all data is processed fairly and lawfully. This means that personal information should only be collected from individuals if employees and councillors have been open and honest about why they want the personal information.

- Data is processed for specified purposes only.
- Data is relevant to what it is needed.
- Data will be monitored so only data that is needed should be held.
- Data is accurate and kept up to date.
- Data is not kept longer than it is needed; data no longer needed will be shredded or securely disposed of.
- Data is kept for a specific purpose only and not because it is or may be considered useful in the future.
- Data is processed in accordance with the rights of individuals; individuals must be informed, if they submit a Subject Access Request (SAR), of all the personal information held about them at no cost unless the request is considered 'manifestly unreasonable'.
- Data is kept securely and confidentially; It cannot be accessed by members of the public.

When the General Data Protection Regulations are introduced on 25th May 2018, Sherfield English parish council will have new obligations to:

- Keep an internal record of all personal data breaches.
- Report any data breeches which may result in a risk to the rights and freedoms of persons to the ICO within 72 hours of the breach being identified and notify the individual affected by the data breach.
- Implement measures to ensure appropriate levels of security against risks presented by processing personal data. Regularly test the effectiveness of these measures.
- Obtain consent via some form of affirmative action to hold personal data.

- Recognise that individuals have the following rights with regards personal data: the right to submit an SAR and be provided with by information held about them within one month of the date of the submission; the right to erasure of their data (within the bounds of practicality for a small organisation); the right to rectification and the assurance that this rectification has taken place; the right to restriction of processing and the right to object to processing.

The risks of noncompliance.

The introduction of the GDPR brings with it significant financial risks in the event of non-compliance and a serious data breach. The capped fines in relation to data protection non-compliance have risen from £500k to €20 million for the most serious of cases. Organisations the size of Sherfield English parish council, together with its employees and councillors could expect similarly significant fines in proportion to the seriousness of the breach or non-compliance.

Sherfield English parish council may wish to consider the following:

1. All councillors advised to have designated email addresses for parish council use only.
2. The council as a whole, operates a 'privacy by default and design' approach to all its working practices to ensure that employees and councillors adhere to GDPR principles.
3. Retention periods for information are implemented going forward.
4. Minutes will not include personal information.
5. Data protection subcommittee to demonstrate compliance.
6. Accept the changes implemented by the GDPR with effect May 25th 2018, recognising that it would not be practical to delete/destroy all historical data with the resources available.
7. Obligations under this policy apply to both employees (the clerk) and councillors.