SHIMPLING PARISH COUNCIL

DATA PROTECTION POLICY

Adopted on 9th July 2018

NB: This policy updated May 2018 to include General Data Protection Regulation (GDPR) 2017

One of the Council's roles is to encourage community involvement and participation; publication of some personal information is integral to this aim. At the same time, such publication must minimise any potential negative impact on individuals, e.g. intrusive marketing or identity theft.

The Council is bound by law to abide by the provisions of the Data Protection Act 1998. The main principles of the act are given at the end of this Policy along with a link to the full online definition of the Act. It should be noted that any individual has the right to make a complaint to the Information Commissioner and that any upheld complaint against the Council could result in a fine.

The simplest way of ensuring compliance is to adopt a simple set of over-arching principles, since individuals acting for the Council may not be familiar with the full Act. The following principles apply:

The following are the eight principles of the Act reproduced from UK Government web site above:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles will be used alongside and in recognition of the GDPR principles:

Principle 1. processed lawfully, fairly and in a transparent manner in relation to individuals;

Principle 2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Principle 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Principle 4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Principle 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Principle 6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As further protection the following recommendations are also advised:

1. Use Copyright

Any paper publication containing personal data should carry the Council's copyright statement (see example at the end of this Policy). Without this, it may be very difficult to control subsequent misuse of the data once published.

2. Take Precautions with Data Published Online

There are always people who will use data from the internet for purposes other than that intended. An example would be gathering contact lists for onward sale; in this case, understanding the demographic or locality of contacts makes them more valuable. The way data is presented online may deter such misuse:

(a) Avoid presenting long lists of personal data. In general, contact information should be "dotted around" and presented in the context of other information.

(b) There is no need to publish email addresses in clear text online. It is better to include them as a "mail hyperlink", e.g. publish "contact John Smith" where clicking this pops up an email window.

The Data Protection Act 1998

For full information see:
http://www.ico.gov.uk/for_organisations/data_protection.aspx

Privacy Statement

The council have published a Privacy Statement in accordance with GDPR and it is available on the council Website

Breaches of the policy or legislation

All breaches of the policy or legislation must be reported immediately to the Proper Officer of the Council and will be reported to the ICO immediately if they contain a possible of actual breach

Retention

All data will be held by the council only as long as necessary or in accordance with Suffolk County Council recommended retention periods. Minutes of council meetings will be held indefinitely.