SOMERFORD PARISH COUNCIL

DATA PROTECTION POLICY

The Parish Council recognises it must at times, keep and process sensitive and personal information concerning both employees and the public. It has adopted this policy to not only meet the legal obligations, but to ensure high standards of practice. The Parish Council is open about its operations and works closely with the community. In the case of information that is not personal or confidential, the Parish Council is prepared to make information available to the public. The types of information which are available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information. The policy is based on these principles:

The Council will make any notifications required to the Information Commissioner's Office under the Data Protection Act and periodically update the information.

DEFINITIONS

For the purposes of this policy, "record" shall be interpreted to mean any papers, files, books, photographs, tapes, films, recordings or other documentary materials or any copies thereof, regardless of physical form, made, produced, executed or received by any employee in connection with the transaction of Somerford Council's business.

The term "electronic record" means any record which is created, received, maintained or stored on local workstations or central servers. Examples include, but are not limited to: email, word processing documents, spreadsheets and databases – including but not limited to file records, investigation reports, financial accounting records and payroll records.

"Official Records" are records maintained but not limited to Accounts (all financial records, VAT records, payroll records, bank accounts etc), electronic records, HR records (personnel records, insurance records etc) and Council Operation records (minutes, correspondence etc).

The Information Commissioner's Office sets out the seven principles of the UK GDPR as:

- Lawfulness, fairness and transparency – the data must be processed in accordance with the law

- Purpose limitation – the data must only be collected for specified legitimate purposes
- Data minimalization – data should only be collected for the purposes for which they are processed
- Accuracy - the data must be accurate or erased or rectified 'without delay'. This is supported by the data subject's 'right to rectification'
- Storage limitation - the data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary
- Integrity and confidentiality - electronic data should be kept in a password protected form or physical data under lock and key
- Accountability – the data controller (i.e. the Council) is responsible for complying with these principles.

Particular attention is paid to the processing of any sensitive personal information and the Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

The Council will provide information on personnel data to employees through the Employee handbook.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have access to that information on request.