Tilney St. Lawrence Parish Council
Data Protection Policy

Introduction

While undertaking its normal business, the Council collects and uses certain types of information about residents of the parish, and others, so that it can carry out its functions. This information includes current, past and prospective employees, suppliers, clients, customers, service users and others.

In addition, it may occasionally be required by law to collect and use certain types of personal information to fulfil its statutory duties.

All personal information held and collected must be dealt with according to the safeguards in the Data Protection Act 1998 (DPA 1998) whether on paper, or other media. Tilney St. Lawrence Parish Council regards the lawful handling of personal information as critical to its successful operation. It is also vital in maintaining confidence between the Council and those with whom it deals.

To this end the Council adheres to the Principles of data protection as stated in the DPA 1998.

The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with eight principles of good practice. These principles are legally enforceable.

The principles require that personal information:

1. Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met;
2. 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. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and “sensitive” personal data.

Personal data means data which relate to a living individual who can be identified:

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller,

and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to:

a) racial or ethnic origin,
b) political opinion,
c) religious or other beliefs,
d) trade union membership,
e) physical or mental health or condition,
f) sexual life,
g) criminal offences or alleged offences.

Handling of personal/sensitive information

The Parish Council will, through appropriate management and the use of strict criteria and controls:

1. Observe fully conditions regarding the fair collection and use of personal information;
2. Meet its legal obligations to specify the purpose for which information is used;
3. Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
4. Ensure the quality of information used;
5. Apply strict checks to determine the length of time information is held;
6. Take appropriate technical and organisational security measures to safeguard personal information;
7. Ensure that personal information is not transferred abroad without suitable safeguards;
8. Ensure that the rights of people about whom the information is held can be fully exercised under the Act. This includes: the right to be informed that processing is being undertaken; the right of access to one's personal information within the statutory 40 days; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information regarded as wrong information.

Responsibilities and Roles

1. The Clerk has specific responsibility for data protection in the organisation.
2. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
3. Documents and any storage media containing paper or electronic material detailing personal information will be held, transported and disposed of with due regard to sensitivity.
4. Confidential paper output no longer required will be shredded before it is included in the recycling process.
5. In legal terms, the overall responsibility for the notification of the Council as a data controller and for ensuring compliance rests with the Parish Clerk.
6. The Clerk and all Councillors are required to be aware of the provisions of the Data Protection Act 1998, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of the Council.
7. Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken or even a criminal prosecution.
8. Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Access to Data

1. An individual is entitled, on making a written request, to be supplied with a copy of all information, with limited exceptions, which forms the personal data held about them.
2. A request for subject access must be responded to within 40 days. If it is not, the individual is entitled to complain to the Information Commissioner.
3. All data subject access requests must be referred to the Parish Clerk, who will co-ordinate the processing of the requests.

Notification to the Information Commissioner

1. The Information Commissioner maintains a public register of data controllers.
2. The Parish Council is registered as such.
3. The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.
4. The Information Officer will review the Data Protection Register annually, prior to notification to the Information Commissioner.
5. Any changes to the register must be notified to the Information Commissioner, within 28 days.
6. To this end, any changes made between reviews will be brought to the attention of the Information Officer immediately.