Sedgefield Town Council

Data Protection Policy Document :

Adopted April 2003

1. Introduction

This policy relates to data protection and the handling of data by Sedgefield Town Council. One of the many concerns regarding data is that liability may arise if the town council misuses that data or unwittingly assists in the process of illegally receiving or giving that data/information to an unauthorized user. The policy not only addresses key issues surrounding data protection but it also sets out STC's policy regarding data protection and handling of information.

With this council being responsible for handling data i.e. the collection and use of personal data by recognizable living individuals STC will be deemed a data controller and therefore must comply with the Data Protection Act 1998.

2. Who is responsible

Anyone handling data/information will be held responsible if any breaches take place. This means that

a. The Town Council can be made liable
b. The Councillors can be held individually and jointly
c. Managers and employees can also be held liable under the principle of precarious liability

3. Data covered by the 1998 Act

The 1998 Act covers the following:

- Any information held on a computer about a living individual who can be identified by or from that data.
- Information held in manual filing systems where it is possible to access specific information about particular people
- Information collected with the intention of storing it on a computer

4. Data Protection Principles

The Town Council must ensure that this policy complies with the following principles laid down by this Act when processing data. This includes: -

- Storage of data
- Collection of data
- Recording the data
- Organising the data
- Consulting the data
- Using data
- Disclosing data
- Destroying data

The eight principles are: -

- Data must be processed fairly and lawfully
- Data must be processed only for specific purposes
- Data must be adequate and relative and not excessive for the purpose for which it is held
- Accuracy is essential
- Data can only be kept for as long as necessary
- Security measures must be appropriate
- Data must not be transferred outside the EU
- Data must be processed according to the data subjects rights

For most instances STC can only process data in the following circumstances: -

- The data subject has given consent to the process in using that data
- Contractual obligations need to be completed with subjects data being processed
- Necessary for public functions or to carry out the interest of the subjects interest
- Legal obligation to process this information
- The processed information is in the legal interest of the subjects or it might by in the legitimate interests of the data controller

5. Sensitive Data

Taking into account that special rules apply, if data is deemed sensitive then both parties must give consent before this may be processed. If sensitive data is being processed i.e. sex life, trade union matters, equal opportunities, medical, check with relevant professional bodies before processing, as they will have guidelines.

6. Data Subject Rights

In the development of any policy the following must be taken into account: -

- The subject's right to object to data being processed
- The subject's right to a full description of the data being held
- Individuals may make a subject access request and a form will be made available stating
- Name of organisation
- Data held
- Description of data
- Purpose for which it is held

7. Implementation/Registration of Data

- Data Protection Act 1998 requires all systems holding data must comply with the new regulations

- All systems set up after 24 October 1998 must comply with the Act unless the Data Protection Commissioners will tell you of your legal position and what you must do regarding registration.

The Policy

1. The name of the person responsible for enforcing this policy is Lesley K Swinbank

2. It is our policy that this data will be used for all council employees providing information on the town council, our council services and operations

3. The town council will consult with groups and individuals and ensure their consent is given before any information is held and used by the town council. Consent to use information will be given in writing where it is reasonably practical to do so.

4. Individuals and bodies that the town council hold information and data on will be given the opportunity to withdraw consent to the town council holding information/data about them.

5. It is the town council's policy to keep a system of individual's consent to data monitoring

6. Anyone who has data held about them on the town council system may have access to that data and records kept by the town council relevant to that individual may inspect that data

7. The town council will ensure that all data is kept secure in either manual or electronic systems

8. Where appropriate, training will be provided on Data Protection for employees and members to ensure that the town council is aware and actively implementing new legislation in this area of the law

9. The town council will notify the Data Protection Commissioner about any data protection processing activities that are not exempt.