MOUNTSORREL PARISH COUNCIL

Data Protection Policy

Introduction

The Parish Council is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000.

The council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

In order to operate efficiently, The Parish Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act to ensure this.

The Parish Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly. To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 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 in particular, 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 is defined as, data relating to a living individual who can be identified from: That data; the 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 is defined as personal data consisting of information as to:
- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Handling of personal/sensitive information

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

- Observe fully conditions regarding the fair collection and use of personal information;

- Meet its legal obligations to specify the purpose for which information is used;

- 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;

- Ensure the quality of information used;

- Apply strict checks to determine the length of time information is held;

- Take appropriate technical and organisational security measures to safeguard personal information;

- Ensure that personal information is not transferred abroad without suitable safeguards;

- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- 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.

In addition, The Parish Council will ensure that:

- There is someone with specific responsibility for data protection in the organisation;

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

- Everyone managing and handling personal information is appropriately trained to do so;

- Everyone managing and handling personal information is appropriately supervised;

- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

- Queries about handling personal information are promptly and courteously dealt with;

- Methods of handling personal information are regularly assessed and evaluated;

- Performance with handling personal information is regularly assessed and evaluated;

- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All staff within the council will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;

- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the council and that individual, company, partner or firm;

- Allow data protection audits by the council of data held on its behalf (if requested);

- Indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by the council will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the council.

Implementation

The council has appointed an Information Officer, namely the Clerk, who will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Information Officer. The Information Officer will also have overall responsibility for:

- The provision of cascade data protection training, for staff within the council.

- For the development of best practice guidelines.

- For carrying out compliance checks to ensure adherence, throughout the Council, with the Data Protection Act.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The Parish Council is registered as such.

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.

The Information Officer will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Information Officer immediately.

Subject Rights

The Act creates rights for those people who have their data stored and also responsibilities for those who store, process or collect personal data. A person who has their data processed by a data controller (the Council in this instance) has a number of rights in relation to the data which is held about them. The person can do the following:

- View the data which is held for a maximum fee of £10;
- Request that information which is incorrect be corrected;
- Require that data is not used in a way which may cause damage or distress;
- Require that their data is not used for direct marketing.

Subject Access Requests

Under section 7 of the Data Protection Act, a person may make a subject access request in relation to information held about them. A person who makes a request and pays a maximum £10 fee is entitled to the following information:

- To be told whether any personal data is being processed;
- A description of the personal data which is held, why the data is being processed and whether this data will be given to any other organisations or people; □
- A copy of the information comprising the data; and
- The source of the data.

Once the Council receives such a request, should the data be disclosable, the request must be dealt with within 40 calendar days of receiving the request. If the personal data which is the subject of the request is normally held for less than 40 days, then the request may be legitimately refused.

How to deal with a Subject Access Request which concerns other people's information

A person may request access to data about them which also carries information regarding a third party. In such circumstances, the Council must assess whether the request can be complied with, without infringing the third party's privacy. For example, if the Council receives a request from an employee to access some personal data and complying with the request would mean disclosing information relating to another individual who can be identified from that information, then the request can be legitimately declined unless the third party consents to the disclosure or it is reasonable for the Council to comply with the request without the third party's consent.

There is an obligation upon a data controller to comply with as much of a request as possible and it may be the case that if you cannot gain consent of the third party and compliance with the request is reasonable, then the Council should consider whether separation the disclosable information from the non disclosable information.

Exceptions

There are circumstances in which a data controller is not obliged to supply certain information to the requester. Some of the most important exemptions apply to:

- Crime prevention and detection;
- Confidential references given by you (but not ones given to you);and
- Information covered by legal professional privilege.