

WINDLESHAM PARISH COUNCIL

Policy and Procedure for Information and Data Protection

A – Data Protection

1 Introduction

- 1.1 The Data Protection Act 1998 regulates the use of personal data and gives effect in UK law to the European Directive on Data Protection. Whereas the Freedom of Information Act 2000 seeks to make information public, the Data Protection Act 1998 seeks to control how information can be processed and used.
- 1.2 The Council is fully committed to compliance with the requirements of the Data Protection Act 1998.

2 Data Protection Act 1998

- 2.1 The Act is concerned with ‘personal data’, that is information about living, identifiable individuals. This need not be particularly sensitive information and can be as little as a name and address.
- 2.2 The Act gives individuals (data subjects) certain rights. It also requires those who record and use personal information (data controllers) to be open about their use of that information and to follow sound and proper practices (the Data Protection Principles.)
- 2.3 Data Controllers are those who control the purpose for which and the manner in which personal data is processed.
- 2.4 Data Subjects are the individuals to whom the personal data relate.
- 2.5 The Information Commissioner is responsible for administering and enforcing the Data Protection Act.

3 Statement of Policy

- 3.1 The Parish Council is required by law to collect and use certain types of information to fulfil its statutory duties and to comply with the requirements of central government.
- 3.2 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; hirers; and suppliers.

3.3 The 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.

3.4 Anyone who obtains and/or records personal information or data about other individuals is a 'data controller' and is thus regulated by the Data Protection Act 1998.

4 Principles of Data Protection

4.1 The Data Protection Act 1998 stipulates that anyone processing data (data controller) must comply with Eight Principles of good practice. These Principles are legally enforceable.

4.2 The Principles require that data:

- 4.2.1 must be processed fairly and lawfully;
- 4.2.2 must be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes;
- 4.2.3 must be relevant, adequate and not excessive for those purposes;
- 4.2.4 must be accurate and, where necessary, kept up to date;
- 4.2.5 must not be kept for longer than necessary;
- 4.2.6 must be processed in accordance with the rights of data subjects under the Data Protection Act.; vii. security precautions must be in place to prevent the loss, destruction or unauthorised disclosure of the data;
- 4.2.7 must not be transferred outside the European Economic Area unless you are satisfied that the country in question can provide an adequate level of security for that data.

5 Sensitive Data

5.1 The Act defines eight categories of sensitive personal data:-

- 5.1.1 the racial or ethnic origin of data subjects;
- 5.1.2 their political opinions;
- 5.1.3 their religious beliefs or other beliefs of a similar nature;
- 5.1.4 whether they are a member of a trade union;
- 5.1.5 their physical or mental health or condition;
- 5.1.6 their sexual life;
- 5.1.7 the commission or alleged commission by them of any offence; or
- 5.1.8 any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

5.2 Since the Council may well hold personal data falling into these categories, the Council will need explicit consent of the individual concerned. The Council will need to ensure that the security is adequate for the protection of sensitive data.

6 Implementation

- 6.1 The Clerk of the Parish Council is responsible for ensuring adherence with the Data Protection Act.
- 6.2 The Information Commissioner maintains a public register of data controllers. The Clerk is a registered data controller on behalf of the Parish Council. The registration is renewed annually.

7 Dealing with subject access requests

- 7.1 If the Clerk receives a written subject access request, it must be dealt with within 40 days from the date of receipt. If further information is required, the 40 days will begin when the Clerk receives the further information. The Council is entitled to ask for a fee of not more than £10 and the 40 days does not begin until this is received.
- 7.2 In response to a subject access request individuals are entitled to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone to whom it may be disclosed, and any information available to you about the source of the data.

B – Information Security

8 Introduction

- 8.1 The purpose of the policy is to ensure the confidentiality, integrity and availability of information is maintained by implementing best practice to minimise risk.

9 Statement of Policy

- 9.1 Information exists in many forms including;
- Printed or written on paper
 - Stored electronically
 - Published on the internet
 - Transmitted by post or electronically
 - Conversational and voice recorded

Information Security requires the adherence to both the Records Management and the Data Protection policies of the Council. Nothing within this policy, or those for Record Management and Data Protection, will detract from the basic principles of the Freedom of Information Act.

10 Implementation

- 10.1 Information Security is primarily vested in the staff employed in the Clerk's Office. However, individual Councillors are also required to meet the objectives of these policies as well as those contained within the Standing Orders and Code of Conduct.

11 Sensitive Data

- 11.1 Where sensitive information is provided, all recipients are expected to respect the nature of such information and afford it the appropriate level of security. Such security will include the prevention of access by unauthorised personnel.

C – Information Requests

12 Introduction

- 12.1 Windlesham Parish Council is committed to the Freedom of Information Act and will meet all obligations so required under it.

13 Statement of Policy

- 13.1 Wherever possible, Windlesham Parish Council will provide additional information beyond the limited requirements of the Act but will be conscious of the Data Protection Act and Copyright
- 13.2 Only ratified Council documents, including approved minutes, will be made available. Draft documents will not normally be made available.
- 13.3 Requests for information may be made in person, by email or letter
- 13.4 Wherever possible, callers will be provided with all permitted information at that time. If this is not possible, they will be informed as to when the information will be available.
- 13.5 Requests by email or letter will be handled in a logical manner. If the information is available on the Parish Council website, those enquiring by email will be so directed.
- 13.6 Where the information is to be provided in hard copy form, the Council reserves the right to make a nominal charge to cover costs.
- 13.7 The Clerk's Office will aim to satisfy all information requests within 5 working days at the latest. Where documents are not yet ratified, the enquirer will be informed of the likely date when they would be available.
- 13.8 A record will be kept of all requests met by hard copy together with the amount charged.

This policy will be reviewed annually or earlier if so required by legislation or additional material