CUCKFIELD PARISH COUNCIL

DATA PROTECTION POLICY

Policy Number 17		
Issue No.	**Date completed**	**Details of amendments**
1	16.09.2016	

1.0 Introduction

1.1 The Data Protection Act 1998 Act 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 seeks to control how information can be processed and used. Councillors and Council staff need to be aware of both regimes and the interplay between them.

1.2 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.

1.3 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). Data controllers are those who control the purpose for which and the manner in which personal data is processed. Data subjects are the individuals to whom the personal data relate.

1.4 The Information Commissioner is responsible for administering and enforcing the Data Protection Act.

2.0 Data Controllers

2.1 As the Parish Council holds personal information about living individuals on paper and on computer (e.g. details of planning applications, grant applications, allotment holders etc.) it is a 'data controller' under the definition of the Act. Accordingly, it has registered with the Information Commissioner's Office (ICO). (Registration No. Z7978504.)

2.2 Where elected members have computers at home and are holding and processing personal data about individuals in the course of undertaking council business, those members will be covered by the Parish Council's notification and those members will have the same responsibilities with regard to data protection as an employee of the Parish Council. (Elected members who process electronic personal data in an individual capacity (i.e. where they are not acting on behalf of the council) are likely to qualify as data controllers and they would individually need to notify the ICO.)

3.0 The Data Protection Principles

3.1 In order to fulfil its obligations under the Act, Cuckfield Parish Council will comply with the eight data protection principles of good practice as set out below:

1 <u>Data must be processed fairly and lawfully</u>
Information will be 'processed fairly and lawfully' and such processing will comply with at least one of the set of specified conditions as set out under the Act and will take cognisance of the additional conditions that apply to sensitive personal data.

2 Data must be obtained only for specific and lawful purposes and not processed in any matter incompatible with those purposes
The council will ensure that there is a legitimate reason for processing data and will, on request provide details of the council, the Data Controller, what will be the intended use of the information and to whom the personal data will be given.

3 Data must be relevant, adequate and not excessive for those purposes
The council will monitor the quantities of data held and ensure that it holds neither too much nor too little and will hold only the data that is actually needed.

4 Data must be accurate and, where necessary, kept up to date.
The council will ensure that personal data will be accurate and if it is not, it will be corrected.

5 Data must not be kept for longer than necessary
In order to comply with this principle, the council will adopt the advice of the National Association of Local Councils with regard to the retention of documents. Only in exceptional circumstances will data be kept indefinitely.

6 Data must be processed in accordance with the rights of data subjects under the Data Protection Act
Upon request and except in very limited circumstances, individuals will be informed, of all the information held about them. The council acknowledges that individuals can prevent the processing of data for direct marketing purposes and are entitled to compensation if they have been caused damage by any contravention of the Act.

7 Security precautions must be in place to prevent the loss, destruction or unauthorised disclosure of the data
The Council will ensure that it provides adequate security for the data taking into account the nature of the data, and the harm to the data subject which could arise from disclosure or loss of the data. A system of passwords will be used to ensure that only staff who are authorised can gain access to personal data.

8 Data must not be transferred outside the European Economic Area.
The council will ensure that this does not occur unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4.0 Sensitive Data

4.1 The Act defines eight categories of sensitive personal data. These are:

(i) the racial or ethnic origin of data subjects;
(ii) their political opinions;
(iii) their religious beliefs or other beliefs of a similar nature;

(iv) whether they are a member of a trade union:
(v) their physical or mental health or condition:
(vi) their sexual life:
(vii) the commission or alleged commission by them of any offence; or
(viii) 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.

4.2 If the council needs to hold personal data falling into these categories it will seek the explicit consent of the individual concerned and will ensure that its security is adequate for the protection of sensitive data.

5.0 Manual Data

5.1 The Data Protection Act 1998 also covers some records held in paper form. Such records need not be notified to the ICO, but will be handled in accordance with the data protection principles.

6.0 Dealing with subject access requests

6.1 If the council receives a written subject access request, it will deal with it promptly, and in any case within 40 days from the date of receipt. (If the council requires further information the 40 days will begin when it receives this further information.)

6.2 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 the council about the source of the data.