

Caterham on the Hill Parish Council

Data Protection Policy

Approved: January 2017

Review date: January 2018

Introduction

The Data Protection Act (DPA) governs the way in which the Council acquires, stores, uses and disposes of personal data. The requirements of the Freedom of information Act are subject to DPA.

Data Protection Principles

More detail may be found at <https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principle>

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

- i. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
 - a. at least one of the conditions in Schedule 2 is met, and
 - b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- ii. Personal data 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.
- iii. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- iv. Personal data shall be accurate and, where necessary, kept up to date.
- v. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- vi. Personal data shall be processed in accordance with the rights of data subjects under this Act.
- vii. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

Responsibilities

Caterham on the Hill Parish Council is registered as a Data Controller. The Clerk, as the Proper Officer of the Council, is responsible for managing the Council's records effectively. The Council as a whole has responsibility for assessing relevant risks and for ensuring appropriate measures are in place. Individual Councillors are responsible for dealing with their casework in accordance with the Council's policies and procedures.

The ways in which Caterham on the Hill Parish Council meets DPA requirements

Mailing and telephone contact lists

This is not sensitive personal data. Lists are maintained by the Clerk, who holds the master. A request to be removed from the list or to amend details is dealt with promptly to prevent further mailings.

Newsletters

Newsletters are sent online to subscribers only. Subscribers manage their own subscription. Access to the data is limited to key administrators, is protected by passwords, and not disclosed to other subscribers.

Information to 3rd parties

The Council does not provide mailing lists to 3rd parties.

Councillor casework

A councillor may hold and disclose personal data to relevant parties when dealing with casework or in the course of their council responsibilities, but this is with the consent of the individual, whose case it is. It is recommended that express permission to disclose is obtained; this is a requirement if the personal data falls in the sensitive category. When the case is closed, any data, including papers, is deposited with the Clerk

Public meetings & Freedom of Information

The names of attendees and speakers in the public forum at Council meetings or the Annual Village Meeting are not recorded in the minutes. Documents requested under the Freedom of Information Act are reviewed to ensure there is no breach of the Data Protection Act

Data collection and analysis

Personal data may be collected occasionally, for example, for the recruitment of volunteers. This is done following current guidelines issued by the Information Commissioner for processing data: <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-2-purposes/>

If data analysis is to be outsourced, the recommended checks are made on the data processor's data protection policy and procedures. The Council does not transfer data outside the European Economic Area. Data when published is anonymised.

Security & Retention of personal data

Data held on the Council's laptop used by the Clerk is protected by the use of a password at computer level and may be further password protected or encrypted for emailing to a

recipient. Councillors take care to ensure 3rd parties e.g. family members, cannot access the council's data and correspondence on their personal electronic devices. Hard copy documents are stored securely and cannot be accessed by 3rd parties.

Complaints

See Complaints policy.

Review

This policy will be reviewed for relevance and current practice annually or following the implementation of significant legislation, and approved by the Council.