

HARDINGTON MANDEVILLE PARISH COUNCIL

Data Protection Policy

1. Introduction

- 1.1 The 1998 Data Protection Act came into force from 1 March 2000. Hardington Mandeville Parish Council supports the objectives of the Act and will comply with it.
- 1.2 The purpose of this Policy Statement is to formalise the position of the Council and state its commitment to maintaining confidentiality of personal information within its record systems. Detailed guidelines are attached as an appendix.

2. Scope

- 2.1 The obligations contained in this Policy Statement apply equally to both Council Members and Employees.

3. Definitions

- 3.1 **Personal Data:** any data that relates to a living individual who can be identified from that data. This includes any expression of opinion about the individual and any indication of the intentions of the Council in respect of the individual.
- 3.2 **Processing:** in relation to information or data, means obtaining, recording or holding the information or data or carrying out set operations on it, including disclosure.
- 3.3 **Data Subject:** an individual who is the subject of personal data.

4. Policy

- 4.1 Hardington Mandeville Parish Council is committed to maintaining the strictest level of confidentiality for any personal data it is responsible for processing. The Council will only process or disclose Personal data for purposes necessary for official Council business and that we have notified to the Data Protection Commissioner. The Council will adhere to the principles outlined in the 1998 Data Protection Act for processing that data.
- 4.2 We will design computer and manual systems to comply with the principles of the Data Protection Act and will train staff involved in processing personal data accordingly. The eight principles are:
 - i) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-
 - at least one of the conditions in Schedule 2 is met, and
 - 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 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.

viii) Personal data shall not be transferred to a country or territory outside of 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.

- 4.3 The Council carries out its affairs in an open manner. Apart from exceptional circumstances as outlined in the Act, we will make information about a data subject available to them, upon request, in an intelligible form.
- 4.4 Where a data subject asks the Council for access to data, the request must come with a fee set by the Council, in accordance with the Act.
- 4.5 The Council will try to hold only the minimum data necessary to perform its business, and will erase or destroy the data in such a manner that confidentiality is maintained. We will try to ensure that data is accurate and up to date, and correct inaccuracies without unnecessary delay.

Adopted by Hardington Mandeville Parish Council on: 16th March 2010

DATA PROTECTION POLICY GUIDELINES

1. Introduction

- 1.1 These guidance notes expand on some of the information in the Council's Data Protection Policy, and you should use the two documents together.
- 1.2 The Data Protection Act 1998 repeals the earlier 1984 Act. The 1984 Act covered data that was "processed by means of equipment operating automatically in response to instructions given for that purpose", i.e. personal data held on computer systems. The 1998 Act widens the description to include "relevant filing systems" or manual data. Relevant filing systems are "structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".
- 1.3 The Act reinforces the principles of confidentiality for personal data.
- 1.4 **Note** - the Act only covers information that relates to living individuals.

2. Responsibilities

- 2.1 The Data Protection Officer will notify the Office of the Data Protection Commissioner of the systems in use and their stated purpose.
- 2.2 New "systems", new uses or changes to "systems" will be notified to the Office of the Data Protection Commissioner before the changes are implemented.
- 2.3 The Data Protection Officer is responsible for ensuring that notifications are up to date and renewals are effectively processed.
- 2.4 Every Member and employee of the Council is responsible for keeping to the Data Protection Act 1998 when processing personal data.

3. System Contents

- 3.1 Only the minimum data necessary to carry out a function will be held.. The information held must be relevant to the purpose. For example some systems allow you to make notes, and these facilities must not be used to record remarks that have no bearing on the purpose of the system, especially if such comments are derogatory or you cannot substantiate them.
- 3.2 Information can be irrelevant if it is held for too long. Information must be both accurate and current. Inaccurate or out of date records must be amended without undue delay.

4. General Access to Personal Data

- 4.1 When you gather information either in writing or verbally it is essential that you tell the data subject what the information will be used for and who else the information may be disclosed to. You cannot then use that information for any other purpose or disclose it to any other individual.
- 4.2 Information must only be provided to the person to whom it relates unless you get prior consent. If information identifies someone else who has not consented to their details being disclosed, you must remove any details identifying the third party before releasing any information.
- 4.3 There is an obvious risk that others may attempt to obtain confidential information relating to someone else. Awareness is particularly important where requests are made over the telephone or if the correspondence address is different from that held on any Council system.

Make checks to verify the identity of the individual. Do this by telephoning the individual back, asking them to confirm something personal such as their account number or by checking an actual signature against others held by the Council.

5. Data Subject Access Request

- 5.1 The Data Protection Act allows individuals to make a Data Subject Access Request. In such a case an individual is entitled to receive, in an intelligible form, all information held relating to them. There are temporary transitional relief periods for manual records that were already in operation before 24 October 1998. Any new processing from that date must comply with the Act immediately.
- 5.2 It is essential that both computer and manual systems are designed in such a way that access requests can be dealt with quickly and effectively.

6. Security

- 6.1 Appropriate measures must be taken to ensure that personal data is secured. In computer operations this includes control over password access and making sure that only authorised persons use the facilities.
- 6.2 Manual records containing personal data should be accessible only to individuals that have legitimate use for the data. Dispose of waste with care. We have procedures to dispose of confidential waste and the facility to shred documents.

7. Disciplinary Action

- 7.1 The Council may consider disciplinary action against any Member or Employee who deliberately disregards any provisions of the Data Protection Policy.
- 7.2 Everyone should also be aware that the Act provides for separate personal liability for any offences in the Act. Where an offence is committed, individuals, as well as the company, may be prosecuted and punished accordingly.