Middleton cum Fordley Parish Council

Information Protection Policy

Adopted: 13 March 2018

1 Purpose

1.1Information is a major asset that the Council has a duty and responsibility to protect.

1.2The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within the Council.

2 Scope

2.1The Information Protection Policy applies to all Councillors, Committees, Working Groups and, Employees of the Council and to contractual third parties and agents of the Council who have access to Information Systems or information used for Council purposes.
For the avoidance of doubt the Policy also applies to the Village Hall Committee and to the Trustees of Middleton Recreation Ground.

2.2Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post or using e-mail or other electronic means
- stored tape or video recordings
- speech

3Information Storage

3.1All electronic information held by the Clerk to the Council will be stored on a computer provided and owned by the Parish Council and which has been configured to allow regular backups to take place and to provide reasonable protection against viruses and hacking. This Policy is based on the understanding that the only electronic information held by the Clerk will continue to be e-mail messages and their attachments, word documents and financial spreadsheets. If other types of application (e.g. data bases) are used in the future then this Policy may need to be extended.

3.2 All electronic information (including e-mail messages and their attachments) held on their personal equipment by Members of the Council should be held only for the purposes of carrying out the business of the Council. Any personal information (including circulation lists etc.) contained therein should not be disclosed to a third party unless agreed by the Data Protection Officer and then only in compliance with the Data Protection Act.

3.3Information will not be held in any form that breaches the Data Protection Act (1998) or formal notification and guidance issued by the Council.

3.4The Council's Document Retention Policy will be followed.

4 Disclosure of Information - Computer and Paper Based

4.1The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is to be reported to the Clerk who will take appropriate action.

4.2Personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4.3Waste computer printed output and other media must be shredded before disposal if they contain personal information.

4.4Distribution of information should be via the most secure method available.

5Disclosure of Information – Telephone, Fax and E-mail

5.1Where this involves the exchange of personal or sensitive information then the following procedures will be applied.

6Telephone calls:

6.1Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.

6.2For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity (this could be passport, driving license, household bill).

6.3Ensure that you are authorised to disclose the information requested.

6.4Ensure that the person is entitled to be given this information.

6.5Ensure that the information you give is accurate and factual.

7Fax transmissions:

7.1Fax should not be used to transmit personal or sensitive information.

8Disclosure of information by email:

8.1When an e-mail message is sent using the public network it may be left at several locations on its journey and could be deliberately intercepted.

8. 2E-mail should not therefore be used for sending personal or sensitive information unless technical measures are in place to keep the message secure (for example by including it in a password protected attachment and communicating the password by a different means).

8.3 The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

9Sharing of Personal Information

9.1Information relating to individuals shall not be shared with other authorities without the agreement of the Data Control Officer.