

Chelveston-cum-Caldecott Parish Council

Data Protection Policy

Ver 2.0

**Adopted under resolution 1007.9
on 12th July 2010**

O/2010/083/MHH

1 Introduction

The *Data Protection Act 1998* (“The Act”) requires anyone who handles personal information to comply with a number of important principles.

The Act also gives legal rights to individuals in respect of personal data processed about them by others.

2 Statement of intent

This policy outlines briefly the main points of the Act and sets out Chelveston-cum-Caldecott Parish Council’s responsibilities in relation to the Act.

3 Scope

This policy applies to all Officers and Councillors of Chelveston-cum-Caldecott Parish Council (“The Council”).

The Council’s responsibilities under the *Freedom of Information Act 2000* are not covered in this policy.

4 Aims, Objectives and outcomes

This policy is intended to maintain the confidentiality, integrity and security of personal data in the Council’s possession.

The principles of good information handling will improve the Council’s reputation by improving confidence in the Council.

5 The Data Protection Policy

5.1 The Data Protection Principles

There are 8 Data Protection Principles (“the Principles”) in the Act sometimes referred to as the principles of “good information handling” which data controllers are required to comply with.

First Principle

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 of the Act is met; and
- in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Act is also met.

Second Principle

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.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Seventh Principle

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.

Eighth Principle

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.

5.2 Individuals' rights

The Act gives rights to individuals in respect of personal data held about them by others. The rights are:

- Right to subject access.
- Right to prevent processing likely to cause damage or distress.
- Right to prevent processing for the purposes of direct marketing.
- Rights in relation to automated decision-taking.
- Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller.
- Right to take action to rectify, block, erase or destroy inaccurate data.

5.3 Exemptions and Modifications

There are a number of exemptions from, and modifications to, various provisions of the Act. These include

- National security (section 28).
- Crime and taxation (section 29).
- Orders made in relation to health, education and social work (section 30).
- Regulatory activity (section 31).
- Processing for the special purposes (section 32).
- Research, history and statistics (section 33).
- Information made available to the public by or under enactment (section 34).
- Disclosures required by law (section 35(1)).
- Disclosures made in connection with legal proceedings (section 35(2)).
- Domestic purposes (section 36).
- Exemptions contained within the *Data Protection (Miscellaneous Subject Access Exemptions) Order 2000* (S.I. no. 419).
- The Miscellaneous Exemptions (Schedule 7) – confidential references given by the data controller.
- Armed forces.
- Judicial appointments and honours.
- Crown employment and Crown or Ministerial appointments.
- Management forecasts / management planning.
- Negotiations.
- Corporate finance.
- Examination scripts.

- Examination marks.
- Legal professional privilege.
- Self-incrimination.
- Transitional exemptions.

5.4 The Information Commissioner's Office

The Information Commissioner's Office (www.ico.gov.uk) is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken.

6. The Council's responsibilities

The Council will observe the good information handling principles as set out in the Act and comply with the legal rights to individuals in respect of personal information processed about them by the Council.

The Council will ensure that personal information is

- Processed fairly and lawfully.
- Processed for specified purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept for longer than is necessary.
- Processed in line with the individual's rights.
- Kept secure.
- Not transferred to countries outside the European Economic Area, unless the information is adequately protected.

The Act requires all organisations to have appropriate security to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage.

Any Officer or Councillor processing personal information must adhere to the guidelines set out below. Also see 6.6 Individuals' Responsibilities.

6.1 Keeping personal information secure

- Keep passwords secure – change regularly.
- Use a screen saver with password protection or log off when away from the computer.
- Dispose of confidential paper waste by shredding.
- Prevent virus attacks by taking care when opening emails and attachments or visiting new websites.
- Keep anti-virus and anti-spyware protection software up to date.
- Securely store hard copy personal information when it is not being used.
- Back-up media (e.g. CD's) will be held in secure storage and routinely destroyed after two years such that the data can not be recovered.

6.2 Meeting the reasonable expectations of the public

- Only collect the personal information you need for a particular Council purpose.
- Update records promptly, for example, change of address.

- Delete personal information the Council no longer requires.
- Check with the Clerk if you are unsure about releasing personal information.

6.3 Disclosing personal information over the telephone

Be aware that there are people who will try and trick you to give out personal information;

- Carry out identity checks before giving out personal information to someone making an incoming call.
- Perform similar checks when making outgoing calls.
- Limit the amount of personal information you give out over the telephone and follow up with written confirmation if necessary.

6.4 Notifying under the Data Protection Act

The Council is registered with the Information Commissioner's Office, for the purposes of

- Provision of Local Services.
- Campaigns, Publications and Fund-raising.
- Staff, agent and contractor administration.

6.5 Handling requests from individuals for their personal information (Subject Access Requests)

The Act gives individuals who are the subject of personal data ("data subjects") a general right of access to the personal data which relates to them.

Requests for access to records and for other information about them are known as 'Subject Access Requests'.

These must be made in writing (including transmission by electronic means) to the Clerk. Any Officer or Councillor receiving a Subject Access Request on behalf of the Council must forward it to the Clerk as soon as practicable in order to meet the statutory timescales for responding.

A fee of £10 will be charged for a Subject Access Request.

On receipt of a Subject Access Request, the Clerk will respond stating whether or not the Council or someone else on the Council's behalf is processing that individual's personal data and if so, the Clerk will provide a description of

- the personal data;
- the purposes for which they are being processed; and
- those to whom they are or may be disclosed.

The Council will also provide, in an intelligible form, all the information which forms any such personal data. This **must** be done within 40 days providing the necessary fee has been paid.

There are circumstances where the Council may withhold information from a data subject, which are set out in the Act, details of which may be found on the Information Commissioner's Office website, www.ico.gov.uk

6.6 Individuals' Responsibilities

Overall responsibility for the efficient administration of the Data Protection legislation lies with the Council and is exercised by the Clerk.

All Officers and Councillors have a duty to comply fully with the *Data Protection Act 1998* as it is a legal requirement.

The Clerk is to report any data loss to the Chairman and Vice-chairman of the Council as soon as practical and to the Full Council at the next meeting.

The Clerk's contract provides that any data held is to be returned to the Council on termination of employment.

Adherence to this Policy is mandatory as good information handling can improve the Council's reputation.

Disciplinary action may be taken against anyone found not to be adhering to this policy.

All Officers and Councillors are expected to ask the Clerk for further clarification or advice regarding Data Protection, if necessary.

Updated to ver.2.0 to include ICO registration classes.

Adopted on 12th July 2010 under resolution 1007.9

Signed

Signed

Chairman of the meeting

Clerk

7. Glossary of terms

Data (including manual data / relevant filing system)

means information which

- is being processed by means of equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should be processed by means of such equipment
- is recorded as part (or with the intention that it should form part) of a relevant filing system; or
- is none of the above but forms part of an accessible record

Personal data

are defined as follows:

“data which relate to a living individual who can be identified:

- from those data; or
- from those data and other information which is in the possession of, or likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual”

Sensitive personal data

The Act defines categories of sensitive personal data, namely personal data consisting of information as to:

- the racial or ethnic origin of the data subject;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a trade union;
- physical or mental health or condition;
- sexual life;
- the commission or alleged commission by the data subject of any offence; or
- any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing,

in relation to personal data, incorporates, amongst other things, the concepts of “obtaining”, “holding”, and “disclosing” data.

Data subject

means an individual who is the subject of personal data. A data subject must be a living individual. Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects.

Data controller

means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor

in relation to personal data, means any person (other than an employee of the data controller) who processes data on behalf of the data controller.

Recipient

in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of the data processor) to whom they are disclosed in the course of processing the data for the data controller.

The term does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Third party

in relation to personal data, means any person other than the data subject,

- the data controller, or
- any data processor or other person authorised to process data for the data controller or processor

The assistance of Mrs Pat Bird, Programme & Information Manager, East Northamptonshire Council, in preparing this policy is gratefully acknowledged.