

THE DATA PROTECTION ACT 1998

GUIDANCE NOTE FOR COMMUNITY COUNCILS

1 Introduction

The Data Protection Act 1998 governs the use of personal data. It imposes important obligations on any persons or organisations, including Community Councils, which acquire, store, use or deal with personal data in any way. Failure to comply with the Act's requirements can have serious legal consequences, including claims for compensation and possible criminal proceedings.

The purpose of this note is to provide Community Councils with information regarding the Act and basic guidance on how to comply with it. More detailed guidance is available from the Information Commissioner (see Part 6 below).

2 Personal Data and Sensitive Personal Data

“Personal data” means any information by which it is possible to identify a living individual (referred to in the Act as a “data subject”). Information on individuals who have died, or on companies or other corporate bodies, is not personal data. But information regarding Community Council members, local residents, individual local authority members or employees, or any other living individual, is personal data.

“Sensitive personal data” means information regarding such things as an individual's racial or ethnic origin, political or religious beliefs, physical or mental health, sexual life and commission of a criminal offence. Special rules apply to sensitive personal data.

The Act regulates the processing of personal data. “Processing” means acquiring data, storing it, amending or augmenting it, disclosing it to third parties, deleting it – ie doing anything with it at all. An individual or organisation which processes personal data is known as the “data controller”.

The Act applies to personal data which is held in any kind of storage system, whether electronic or manual.

3 The Data Protection Principles

The Act sets out some basic rules regarding processing personal data, known as the Data Protection Principles. These include –

- Data must be processed fairly and lawfully;
- Data must be obtained for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes;
- Data must be adequate, relevant and not excessive;
- Data must be accurate and kept up to date;
- Data must not be kept longer than necessary;
- Data must be processed in accordance with the data subject's rights;
- Appropriate technical and organisational measures must be taken against the data's unauthorised or unlawful use and their accidental loss, damage or destruction.

4 Data Subjects' Rights

The Act gives important rights to data subjects, including the right –

- To be informed that their personal data is being processed by the data controller;
- To be given access to their personal data;
- To require their personal data not to be used for direct marketing purposes;
- To require the data controller to stop any processing of their personal data which is causing substantial and unwarranted damage or distress.

5 Contravention of the Act

If a data controller contravenes the Act, compensation may be payable to any person who suffers damage and distress because of that contravention. In some circumstances, contravention of the Act may also be a criminal offence, for which a fine may be payable.

6 The Information Commissioner

The Act is regulated and enforced by the Information Commissioner (not to be confused with the Scottish Information Commissioner, who enforces the Freedom of Information (Scotland) Act 2002). The Commissioner has powers under the Act to issue notices to data controllers, requiring them to provide him with information regarding their compliance with the Act, or to carry out certain steps under the Act. He also has power to carry out investigations, including the power to enter data controllers' premises.

The Information Commissioner's Office – Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT

The Commissioner publishes detailed guidance on various aspects of the Act. That guidance is available on the Commissioner's website at <https://ico.org.uk/about-the-ico/who-we-are/scotland-office/>.

7 Notification to the Information Commissioner

All data controllers are obliged by the Act to notify the Information Commissioner of the classes of personal data which they are processing, the purposes for which they are processed and the recipients to which the data may be disclosed. This information is included in the Commissioner's Register of Notifications, which is open to public inspection. It is a criminal offence to process personal data without first notifying the Commissioner.

8 Complying with the Data Protection Act

To comply with the Act, Community Councils should take the following steps –

- 8.1 Nominate an office bearer (eg the Secretary) as the person responsible for data protection. In many organisations, this person is referred to as the Data Protection Officer.

- 8.2 Carry out a data protection audit – identify what personal data are held and who the data subjects are; ascertain the purposes for which the data are to be used; identify where and how the data are stored or recorded.
- 8.3 Inform the data subjects in writing (a) that their personal data are held, and (b) the purposes for which the data are used.
- 8.4 Ensure that personal data is properly protected – if data are stored electronically, ensure that they are password-protected and (in sensitive cases) encrypted. If they are stored manually (eg a paper filing system), ensure that the files are kept in a secure place.
- 8.5 Ensure that personal data is never disclosed to any unauthorised third party, whether accidentally or on purpose.
- 8.6 Periodically review the personal data that are held, making sure that they remain accurate and up to date – where necessary dispose of data that are no longer needed.
- 8.7 The Information Commissioner must be notified of the personal data being processing, the purpose and the recipients to which the data may be disclosed. It is a criminal offence to process personal data without having first notified the Commissioner.

Notification can be done on-line at the Commissioner's website, by going to www.ico.gov.uk/what_we_cover/data_protection/notification.aspx and then by following the step-by-step directions given there. The website includes standard templates for different types of organisations, including a set of local and central government templates; this includes, in turn, standard template N870 – Council (Parish and Community Councils). By clicking on that template, the standard classes and uses of personal data for Community Council are automatically included in the notification, which can then be printed, signed and sent by post to the Commissioner.

Notification costs £40 and must be renewed annually.