DATA PROTECTION GUIDANCE FOR COMMUNITY COUNCILS

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 either electronically or within certain paper records. Whilst failure to comply with the Act's requirements can have serious legal consequences, Community Councillors should be reassured that most breaches are likely to simply require remedial action to be undertaken and would not be deemed to be criminal offences.

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

Special rules govern the processing of sensitive personal information.

"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

"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 and Community Councils should seek advice if they hold any sensitive personal data (other than that which is in the public domain such as the political affiliation of local elected members or the denominations of clergy).

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 – i.e. 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

A breach of the Data Protection Principles is not a criminal offence in itself although this may change in the near future. Current offences include the unlawful obtaining, disclosing or selling of information, a failure to follow a Notice from the Commissioner and the failure to notify the Commissioner of processing which takes place. These offences are punishable by the payment of a fine.

Compensation may be payable to any person who suffers damage and distress as a result of a contravention of the Act. Such compensation is awarded by the Court.

6 The Information Commissioner

The Data Protection Act is regulated and enforced by the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF and applies throughout the UK. 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; as indicated above, failure to comply with a Notice is a criminal offence. He also has power to carry out investigations, including the power to enter data controllers' premises.

The Commissioner publishes detailed guidance on various aspects of the Act on his website at www.ico.gov.uk . Advice can also be obtained from his Scottish office in Edinburgh at Scotland@ico.gsi.gov.uk or 0131 225 6341 (The Information Commissioner should not be confused with the Scottish Information Commissioner, who enforces the Freedom of Information (Scotland) Act 2002.)

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. Community Councils only need to notify if personal data are processed electronically. This information is included in the Commissioner's Register of Notifications, which is open to public inspection. Unless within an exempt category, it is a criminal offence to process personal data without first notifying the Commissioner. It is likely that only a few Community Councils will be covered by an exemption.

8 Complying with the Data Protection Act

It is likely that community councils must comply with the Data Protection Act because they process personal data as defined under the Act. For example, it is likely that the Secretary of Community Councils will hold electronic records of contact details of its members, of some local residents and of elected members or employees of the local authority. These may be within databases, Minutes of meetings or in correspondence

In order to comply with the Act, Community Councils should take the following steps

8.1 Nominate someone (eg the Secretary) as the person responsible for data protection.

8.2 If collecting personal data from individuals, you should explain the purpose for which the data is being collected as well as giving them the name of the Community Council and the name of the person nominated as being responsible for data protection.

8.3 Ensure that personal data are 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.

8.4 Ensure that personal data are never disclosed to any unauthorised third party, whether accidentally or on purpose. Do not discuss personal issues in public or leave papers or computer files unsecured at home.

8.5 Periodically review the personal data that are held, making sure that they remain accurate and up to date – where necessary dispose of or shred data that are no longer needed.

8.6 VERY IMPORTANT: notify the Information Commissioner of the personal data which are being processing, the purposes for which they are processed 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.

Before notifying, 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. This will assist in completing the notification template.

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 N958 – Scottish Community Council . By clicking on that template, the standard classes and uses of personal data for Community Council are automatically included in the notification. Check the details and modify the form before printing it off, signing and posting to the Commissioner.

Alternatively, a Community Council may send the required information, as shown below, to - notification@ico.gov.uk, and ask for a template for a Scottish Community Council to be completed. The Information Commissioner's Notification Department will then provide a draft for the Community Council to approve/amend as necessary.

Community Councils can also phone the Information Commissioner's Notification Helpline on **01625 545 740** and ask for a draft template for a Scottish Community Council to be completed. The required information (as shown below) should be given over the phone.

The information needed is as follows:

- Community Council name
- Community Council address

- Contact name and role in the Community Council (i.e. Chair/Secretary/Treasurer)
- Contact address
- Contact telephone number
- Contact fax (if available)
- Contact e-mail address

Notification costs £35 and must be renewed annually.