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 Inaccurate or out of date records must be amended without undue delay.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.