DUNDEE CITY COUNCIL

DATA PROTECTION POLICY

1. Dundee City Council (hereinafter referred to as "the Council") supports the objectives of the Data Protection Act, 1998 (hereinafter referred to as "the Act) and intends to retain its presents policy of maintaining the confidentiality of personal information processed automatically (on computers etc) and held on manual files which are considered to be "relevant filing systems" in terms of the Act.

2. The Council expects all elected members and employees to comply fully with this policy and the Date Protection Principles (Appendix I).

3. The Council will hold the minimum personal information necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate and up-to-date, and that inaccuracies are corrected without unnecessary delay.

4. Personal information is confidential. Automated systems and relevant filing systems will be designed to comply with the Date Protection Principles. Personal information will be disclosed only for registered purposes to:

   - Council staff where such information is vital to their work;
   - others as detailed in the Registration;
   - the Court under the direction of a Court Order.

5. It is the responsibility of Directors and Heads of Department to ensure compliance with this policy. All systems within their Division or Department containing information about individuals must be identified, made secure, and notified to the Data Protection Officer for notification purposes. It is the responsibility of all employees to co-operate in this task. Upon discovering that the Council's Policy on Data Protection is not being complied with, the Chief Executive, after consultation with the Director of Finance, shall have full authority to take such immediate steps as considered necessary.

6. The Council will provide to any individual who requests it in the proper manner a written copy in clear language of the current information held. The Council shall fix a fee for this service which in appropriate circumstances may be waived by the Chief Executive. Employees of the Council will not be required to pay any such fee when requesting access to information regarding their employment.

7. In cases where the Council acts as a bureau providing services to outside organisations, no disclosure will be made without the written consent of the third party except under the direction of a Court Order checked by the Chief Executive.

8. All employees of the Council must comply with the requirements specified in the Council's e-mail/internet guidelines.

9. Disciplinary action may be taken against any Council employee for deliberate or reckless breach of any instructions contained in, or following from this Date Protection Policy.

October 2001

APPENDIX

DATA PROTECTION ACT 1998

THE DATA PROTECTION PRINCIPLES

1. 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.

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with the purpose or those purposes.

3. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

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

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

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

7. 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.

8. 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.