Data Protection Policy

This document sets out Epsom & Ewell Borough Council's policy regarding data protection. The Data Protection Acts 1984 and 1998 and the EC Data Protection Directive form the background to the document. The Policy is drafted using the terms of the **Data Protection Act 1998**, the **Freedom of Information Act** and the **Human Rights Act 1998.**

Table of Contents

1. Introduction

The purpose of the data protection legislation is to regulate the way in which personal information about individuals, whether held on computer or in a manual filing system, is obtained, stored, used and disclosed. The legislation grants rights to individuals, to see the data stored about them and to require modification of the data if it is wrong and in certain cases, to compensation. The provisions amount to a right of privacy for the individual.

The Data Protection Act 1998 presented a number of significant challenges for local authorities. There was the extension of the scope of data protection from purely automated records to certain types of paper and other manual records and new rules that required that data controllers established a legitimate basis for the processing of personal data; and there were significant changes to the system of registration that existed under the 1984 Act.

The 1998 Act required all processing of personal data to be notified to the Data Protection Commissioner and to be kept and used in accordance with the provisions of the Act.

2. Definitions

To aid the understanding of this document and the provisions of the Data Protection Act the following definitions are provided for assistance:

Data
is information that is:

- being processed by means of equipment operating automatically in response to instructions given for that purpose (e.g. payroll system)
- recorded with the intention that it should be processed by means of such equipment
- recorded as part of a manual filing system or with the intention that it should form part of a **relevant filing system** (see definition below)
- one of a number of records to which public access is allowed.

Data Controller
means the Council as the organisation who determines how data is processed.

Data Processor
means any person, other than an employee of the Council, who processes data on behalf of the data controller (e.g. someone contracted to the Council to print documents containing personal data).

Data Subject
is the individual about whom personal data is held.

Personal Data
means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, and any indication of the intentions of the data controller or any other in respect of that individual.

Sensitive Personal Data
means personal data consisting of information as to:-

- racial or ethnic origin of the data subject
- his/her political opinion
- his or her religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- his or her physical or mental health or condition
- his or her sexual life
- the commission or alleged commission by him or her of an offence
- any proceedings for any offence committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing
is very widely drawn and means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:

- organisation, adaptation or alteration
- retrieval, consultation or use
- disclosure

- destruction

of the information or data.

Relevant Filing System
means any data that is recorded as part of a manual filing system or with the intention that it should form part of a relevant filing system (e.g. "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is 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").

3. Principles

The Data Protection Act 1998 contains 8 governing Principles relating to the collection, use, processing and disclosure of data, and the rights of data subjects to have access to personal data concerning themselves. These Principles are detailed below.

- Personal data shall be **processed fairly and lawfully** and, in particular shall not be processed unless one of the conditions in Schedule 2 is met. These can be summarised as consent, contract, legal obligation, vital interests, public interest and balance of interest. In the case of sensitive personal data at least one of the conditions in Schedule 3 must also be met, which can be summarised as explicit consent, employment law, vital interests, non-profit associations, manifestly made public, legal claims, justice/statute Crown, medical purposes, ethnic monitoring.
- Personal data shall be obtained only for **one or more specified and lawful purpose** and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.
- Personal data shall be **accurate** and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes **shall not be kept for longer than is necessary** for that purpose or purposes.
- Personal data shall be processed **in accordance with the rights of the data subject** under this act (this includes the rights of subjects to access the data and to correct it).
- 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 (this relates to data security).
- 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.

These principles are required as the minimum standards of practice for any organisation with respect to personal data.

4. Policy

The Council supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed either on computer or in manual files and to increase the access given to individuals to information relating to them.

The Policy links to the other Council policies such as IT Security, Information Assurance and HR policies.

It also links to the Surrey Information Sharing Protocol. Data may also be shared with certain other public authorities in accordance with statutory and other requirements (see **Disclosures**).

External and Internal Registration / Notification

The Council has an external registration/notification with the Information Commissioner. The Register can be searched at http://www.ico.gov.uk/ The EEBC Registration references are:

- **Z7075379** Epsom & Ewell Borough Council (renewable every 29 August)
- **Z6255830** Electoral Registrar of Epsom & Ewell Borough Council (renewable every 1 March)

The Register Entry gives general descriptions of the type of data processing activities carried out by Local Government. The Register Entry is therefore supplemented by an internal register of data repositories, maintained by the Data Protection Officer.

Amount of data to be held

The Council will hold the minimum personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

Subject Access

The Council will provide to any individual who requests it, in a specified manner, a reply stating whether or not the Council holds personal data about that individual. A written copy, in clear language, of the current data held, will be given. A fee will not be levied for this service.

However, there are certain exemptions from the right of subject access, which relate largely to a test of prejudice. For example, personal data that are held for the purpose of the prevention or detection of crime are exempt, to the extent that providing access would be likely to prejudice that purpose. In addition, data may be withheld if it is not possible to release information without disclosure of personal data about other people.

Public Registers

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals. Strict compliance with the legislation giving rights of access will be used in all cases.

Disclosures

Disclosures of information must be in accordance with the provisions of the Act and the Council's registration/notification. Where the Council has a duty to disclose certain data to public authorities (such as the Inland Revenue, Customs and Excise, Benefits agency), this will be done in accordance with statutory and other requirements.

Legal and internal rules limit disclosure within the authority either to council officers or elected members. When a request for information is made, the minimum of personal data will be made available on a need to know basis.

System Design

The Council intends that personal data must be treated as confidential. Computer systems are and will continue to be designed to comply with the Principles of the Data Protection Act so that access to personal data should be restricted to identifiable system users.

Training

It is the aim of the Council that all staff will be fully informed of their obligations under the Data Protection Acts and aware of their personal liabilities, and where appropriate further training will be given.

Disciplinary Action
The Council expects all of its staff and members to comply fully with this Policy and the Principles of the Data Protection legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures following from this policy.

5. Responsibilities

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

Day to day responsibility for administration and compliance with the act is delegated to **Directors and Division Heads**, for compliance with the Act's provisions within their respective areas of authority. In some cases, this may involve a joint responsibility (for example, where one Division, such as Customer Services, works on behalf of another Division).

All **Officers** and **Members (Councillors)** have a duty to observe the Principles of the Act and the procedures referred to in this document.

Please note: **Councillors** could be regarded as data controllers if they process personal data either manually or by computer, whether on their own equipment or on equipment provided to them by their local authority. Just as any other individual holding and processing personal information about others, Councillors need to comply with the Data Protection Act, and need to notify the Information Commissioner of all purposes for which they hold and process personal data.

However, where holding and processing personal data about individuals *in the course of undertaking Council business*, the elected member will be covered by the authority's notification, and have the same responsibilities in respect of data protection as an employee of the authority.

Further guidance on **Data Protection for Councillors** can be found in the document of that name which has been published by the Improvement & Development Agency (I&DeA). Their website can be found at http://www.idea.gov.uk/, and the article (issued 16 August 2001) is to be found in their News Articles.

Individuals who do not handle data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.