

REIGATE & BANSTEAD BC

Corporate Policy for the Data Protection Act 1998



INTRODUCTION

It is the policy of this Council to comply fully with the Data Protection Act 1998 and other related legislation. The purpose of the Act is to regulate the use of automatically processed information, and manual paper-based files, that contain **personal information** relating to individuals, and the provision of services in respect of such information.

This policy applies to all employees, including contractors, of Reigate and Banstead Borough Council.

PURPOSE

The purpose of this policy is to ensure that all staff are aware of their individual responsibilities in relation to Data Protection within the Council and to identify the rules governing access to personal information about individuals held by the Council.

RESPONSIBILITIES

The Council recognises its duty to handle personal data in a proper and confidential manner at all times. This duty covers:

- obtaining
- storage and security
- use
- maintenance
- disclosure
- disposal and destruction

It is the responsibility of each and every employee of the Council to comply with this policy.

It is the responsibility of the Data Protection Officer to:

- enforce the policy on behalf of the Lead Officer of the Council
- ensure that the Council maintains its registration under the Data Protection Act 1998
- update that registration where appropriate
- ensure compliance with the Data Protection Act requirements.

It is a requirement of the Act that all **data controllers** notify the **Information Commissioner** of certain details relating to personal data which they hold and

process. These details include the purpose for which the data is being held, the categories of data subjects to which the data relate, the classes of data being obtained and held and the categories of persons or organisations to which the data may be disclosed.

The Council has a responsibility to ensure that **data subjects** have proper access to information that the Council holds regarding them, provided that a written request is received and the appropriate fee is paid.

DATA PROTECTION ACT 1998

The protection of personal information about living individuals is a requirement of law. The Data Protection Act 1998 received royal assent in July 1998 and its full provisions came into force from 1st March 2000. The Act is designed to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The Act incorporates and builds upon the previous 1984 Data Protection Act.

The Act gives protection to individuals about whom data is recorded either manually or electronically. Any individual has a right to see what information is held about them and may challenge this information if they feel it is inaccurate or has caused damage to themselves.

The Act places obligations on those who record and use information about individuals. They must register the use of that information (through the Information Commissioner) and they must ensure that they follow sound practises in recording and using the information, in line with the Data Protection Principles.

The Data Protection Act 1998 covers all information that is held on computers or computer media), and any set of manual information relating to individuals to the extent that 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.

DATA PROTECTION PRINCIPLES

The Data Protection Act states that all data controllers must comply with the following Data Protection Principles.

- 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -**
 - (a) at least one of the conditions in schedule 2 is met;**
 - (b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.**
- 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**
- 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

- 4. Personal data shall be accurate and, where necessary, kept up to date.**
- 5. Personal data processed 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 or 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 or protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

Compliance with the eight principles of the Data Protection Act 1998 is enforceable under the legislation.

INDIVIDUALS RIGHTS

The Act gives rights to individuals in respect of personal data held about them by others, these are;

- Right of subject access.
- Right to prevent processing likely to cause damage or distress.
- Right to prevent processing for the purposes of direct marketing.
- Rights in relation to automated decision taking.
- Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller
- Right to take action to rectify, block, erase or destroy inaccurate data.
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

INFORMATION THAT MUST BE PROVIDED TO INDIVIDUALS

Principle 1 of the Data Protection Act places a requirement on the Council to ensure that data is processed fairly and lawfully. For this to take place, the Council is required to supply certain information to individuals about whom it holds data. It is the responsibility of all Council employees who obtain information about individuals on behalf of the Council to ensure that those individuals have been provided with the following information;

- The identity of the data controller: (Reigate and Banstead Borough Council).
- The nominated representative of the Council for the purposes of the Data Protection Act (Data Protection Officer).
- The purpose or purposes for which the data are intended to be processed.
- Any further information which is necessary, having regard to the specific circumstances in which the data are to be processed, to enable the processing to be fair. eg who information may be disclosed to and for what purpose.

It is the responsibility of the (*insert department or individual responsible*) to ensure that appropriate information regarding the Council's registration under the Data Protection Act, its uses of information and information regarding access requests is displayed in all Council premises.

RIGHT OF SUBJECT ACCESS

All individuals have the right upon making a request in writing and paying the appropriate fee, to be told by the Council; whether it or someone else on its behalf is processing personal data relating to that individual.

Individuals have the right to be given:

- a description of the personal data the Council holds;
- the purposes for which it is being processed; and
- those to whom it is, or may be, disclosed.
- a copy of the information about them held by the Trust, except where the supply of such a copy is not possible or would involve disproportionate effort, or the individual agrees otherwise. The copy supplied must be in an intelligible form, i.e. if codes are used, explanations of what these codes are must also be supplied.
- information as to the source of the personal data if available, except where this would involve the disclosure of information relating to an individual other than the subject of the information (A third party), including the fact that they were the source of the information. A disclosure of this nature may only take place where;
- the other individual has consented to the disclosure of the information, or
- where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

All requests for subject access must follow the procedure at Appendix 1.

OBLIGATIONS

In compliance with the Act, the Council will:

- acknowledge the rights of individuals relating to personal data and ensure that these rights can be exercised as specified in the Act.
- ensure that personal data is obtained fairly and lawfully.
- ensure that personal data will only be processed for the purposes specified in the relevant notification to the Information Commissioner.
- obtain and process data in a confidential manner ensuring that data is fit for the purposes specified, is not excessive and is disposed of when no longer required (subject to any statutory requirements).
- ensure that necessary and sufficient steps are taken to ensure that the data is accurate and up-to-date.
- ensure that necessary and sufficient security measures are in place to protect data against damage, loss, misuse or inappropriate disclosure.
- ensure that transfer of data is done in a lawful manner with due regard for security.

ACTIONS

To discharge its obligations within the DP Act, the Council will:

- ensure that Service Managers are fully aware of their responsibilities under the Act for all personal data held within their units and have clear procedures for the collecting, processing, access and security of the data.
- maintain the corporate post of Data Protection Officer (DPO) who will have overall responsibility for day-to-day compliance with the Act and for liaison with nominated data 'managers' to manage corporate data responsibly.
- ensure that staffing resources are available within Service Units for a responsible data protection 'manager' in each Service Unit who will be responsible for co-ordinating the tasks necessary to ensure compliance with the DP Act and other related legislation.
- ensure that employees (and others acting on behalf of the Council) understand their responsibilities under the Act and that regular, appropriate training or instruction is given for this purpose.
- ensure detailed procedure notes are incorporated into office working practices for proper creation, collection, processing and disclosure of data.
- ensure that employees (and others acting on behalf of the Council) have access only to personal data that is necessary for the performance of their duties.
- ensure that disclosure of personal data to third parties is controlled and restricted to those recipients registered.
- ensure that **subject access** requests to personal data are dealt with in a courteous and timely manner whilst ensuring that the data subject (or authorised representative) does have a legitimate right to access the information.
- review annually all notifications lodged with the Information Commissioner to ensure that they are relevant, efficient and effective.
- notify the Information Commissioner within 28 days of the register entry becoming invalid.
- charge a maximum charge of £10 for each disclosure request from data subjects on written request to the Data Protection Officer.
- ensure that individuals are made aware of the proposed uses and disclosures of personal data at the point of collection.

GLOSSARY OF TERMS

PERSONAL INFORMATION: is

Data which relates to a living individual who can be identified from those data and other information which is, or is likely to come into the possession of the data controller, and includes any expression of opinion and any indication of the intention of the data controller, or any other person, in respect of the individual. Personal information that is held by the Council and subject to the provisions of the Data Protection Act includes information about employees and Councillors, as well as clients of the Council.

DATA CONTROLLER : is

An individual or organisation who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data is processed.

DATA SUBJECT: is

an individual who is the subject of personal data.

INFORMATION COMMISSIONER:

The Commissioner is an independent supervisory authority and has an international role as well as a national one. In the UK the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed

DISCLOSURE IS : is

The passing of personal data to a third party, either an individual or an organisation.

DP NOTIFICATION : is

The means of updating the official public register of the purposes for keeping personal data in the Council. It also includes descriptions of the data collected, the class of person the data relates to and to whom the personal data can be disclosed.

SUBJECT ACCESS : is

The right of a data subject to have access to the information held about them.

THIRD PARTY : is

Any person other than:-

- a) the data subject,
- b) the data controller or
- c) any data processor or other person authorised to process data for the data controller or processor.

The expression third party does not include employees or agents of the data controller.