

# Ealing Council Data Protection Policy



## Foreword

The London Borough of Ealing is committed to ensuring the privacy of the individual is respected and that all personal data that is processed by the organisation is dealt with in accordance with the Principles of the Data Protection Act 1998 (the "Act").

The Act is designed to safeguard personal data and allow organisations such as the Council to collect and process this data for legitimate purposes.

All Council employees need to ensure that other people's information is protected and kept safe at all times. If personal information is taken from one location to another it must be done so as a necessity and not as a convenience and it must be done so in the safest possible way. We must ensure equipment is fully password protected and encrypted, and kept secure at all times. Files, diaries, notepads or computer equipment must never be left unattended.

Any queries about Data Protection employee obligations or the rights of individuals and members of the public in relation to information about themselves should be directed to the Corporate Data Protection team.

Corporate Information and Data Protection Manager  
February 2012

# Introduction

The Council needs to collect and use personal data about individuals, residents, customers, employees (present, past and prospective), suppliers, contractors and other businesses, in order to meet its statutory obligations and provide its services. No matter how personal data is collected or held, either manually or electronically, it must be handled and processed properly to ensure that the Council meets its legal obligation to comply with the principles of the Data Protection Act 1998 (the Act).

The Act places obligations on organisations, such as the Council, which process<sup>1</sup> personal data<sup>2</sup>, and protects the rights and freedoms of the individuals who are subjects of that data.

## Purpose

The purpose of this policy is to:

- explain the Council's commitment to the lawful and fair treatment of personal data and its intent to comply with the principles of the Act.
- ensure that all personnel, elected members<sup>3</sup> and partners<sup>4</sup> are made aware of their responsibilities under the Act; and
- ensure that all employees, elected members and partners are aware of the rights of data subjects,<sup>5</sup> and ensure that those rights are protected.

## Scope

This policy applies to all personnel whether employed directly by the Council or by a "partner", members and any other individual who has access to personal data collected, owned and used by the Council.

## The Council's Commitment

The Council, through the appropriate application of managerial and operational controls, will:

- only process personal data fairly and lawfully and fully observe all required conditions in the fair collection and use of personal data;
- at all times specify the purpose(s) for which personal data is being used;
- only collect the personal data that is necessary to fulfil the operational needs of any service provided or to comply with legislative requirements;
- take steps to ensure the quality and integrity of personal data used;
- put in place the appropriate measures to ensure that personal data is only retained for as long as it is needed for the purpose(s) it was obtained for, or to meet legal requirements;
- ensure that the rights of every individual who provides the Council with personal data are respected;
- provide the appropriate technical and organisational security measures that will safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction or damage;
- ensure that personal data is not transferred outside the European Economic Area without the appropriate safeguards.

In addition to the above the Council will endeavour, through the distribution of guidance material and training, to ensure that:

---

<sup>1</sup> Processing in relation to data includes obtaining, recording, holding, using or disclosing,

<sup>2</sup> Personal data is data that relates to an identifiable living individual.

<sup>3</sup> Elected members need to understand in what capacity they are acting under the provisions of the Act

<sup>4</sup> A partner includes contractors, consultants, agency staff, service providers etc.

<sup>5</sup> A data subject is an individual to whom the data relates.

- all processing of personal data undertaken by the Council is notified to the Information Commissioner's Office;
- all employees managing and handling personal data are aware of and understand their responsibilities under the Act;
- every individual managing and handling personal data is appropriately trained to do so;
- every individual understands the purpose(s) for which they are processing personal data and also under what circumstances further processing may take place;
- every individual managing and handling personal data understands the rights of the data subject;
- there is a post with overall responsibility for the monitoring of data protection legislation and compliance within the Council;
- there is a representative within each department/service to provide a communications network to ensure compliance with the Act.

## Employee & Member Responsibility

All Council personnel are personally responsible and accountable for ensuring compliance with the principles of the Act and that their use and handling of personal data is in accordance with the purpose(s) the Council have notified to the Information Commissioner. Adherence to the Act forms part of Council's Code of Conduct and contract of employment.

Any personnel or member who fails to carry out their duty in compliance with the Act will be subject to disciplinary action.

All managers must ensure that any additional or new purpose for which they are processing personal data is notified to the Corporate Data Protection Manager, who will amend the Council's notification as appropriate.

## Individual Rights

The Act gives rights to individuals in respect of personal data processed about them by the Council. These rights apply to all individuals, whether they are employees, elected members or members of the public. The Data Protection Act confers the following rights on data subjects:

- the right of access to personal data;
- the right to prevent processing likely to cause damage or distress;
- the right to prevent processing for purposes of direct marketing;
- rights in relation to automatic decision-taking;
- the right to compensation for failure by the Council to comply with the requirements of the Act;
- the right, via the courts, to rectify block, erase, or destroy inaccurate data; and
- the right to request an assessment, by the Information Commissioner, that the processing of personal data is in compliance with the Act.

## Right of access

Subject to a limited number of exemptions, an individual has the right to be supplied with a copy of their personal data. This is called the subject access right and is the right that individuals are most likely to make use of. Requests must be in writing and the Council has 40 days in which to comply with the request.

All personnel should be able to recognise a request when received and be aware of the procedure for handling such requests (see the Intranet). If an employee is instructed to prepare a file in accordance with Section 7 of the Act they should be suitably trained and respond within the statutory time period.

# The Information Commissioner's Office

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessment to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specific information within a certain time period;
- Service enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specific steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing or personal data follows good practice; and
- Report to Parliament on data protection issues of concern.

Appeals from Notices are heard by the Information Tribunal, an independent body set up specifically to hear cases concerning enforcement notices or decision notices issued by the Information Commissioner.

In April 2010 the ICO gained powers to fine and penalise organisations which fail to comply with the Act. These powers are few reaching and have significant implications for failure.

## Criminal Offences

The Act creates a number of criminal offences. Failure to comply with the requirements of the Act could result in personnel being held liable under the Act for their actions.

The Act also provides for separate personal liability of directors and other staff where their consent, connivance or neglect has been instrumental in an offence committed by the corporate body.

All personnel should be aware that if found guilty of committing an offence under the Act, they could be liable for a fine of up to £5,000 in a Magistrates court or an unlimited fine in a Crown court.

## The Data Protection Principles

There are **eight** Data Protection principles that must be adhered to. The following is a summary:

1. Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary kept up-to-date;
5. Personal data shall not be kept for longer than is necessary;
6. Personal data shall be processed in accordance with the rights of the data subject;
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, 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 adequate levels of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

<b>Release:</b>	Published
<b>Date Reviewed:</b>	01/01/2012 01/01/2013
<b>Job Title:</b>	Corporate Data Protection Manager
<b>Owner:</b>	Ealing Council