

# Data Protection Policy

*London Borough of Barnet*

**Document Control**

<b>Document Description</b>	Data Protection Policy		
<b>Version</b>	V.001		
<b>Date Created</b>	30 July 2009		
<b>Status</b>	Final – Signed off by Directors Group		
<b>Authorisation</b>	Name	Signature	Date
<b>Prepared By:</b>	Lucy Wicks		
<b>Checked By</b>	Sian Hughes Jeff Lustig Niall Toru Victoria Gray		

**Version Control**

<b>Version number</b>	<b>Date</b>	<b>Author</b>	<b>Reason for New Version</b>
V.001	30/07/09	L Wicks	Initial draft
V.002	01/09/09	L Wicks	Checked by Legal Services and passed to JEL for comment

*Date last reviewed:* November 2010  
*Date of next review:* November 2011

## 1. Introduction

This policy is in place to ensure that the London Borough of Barnet (“the Council”) complies fully with its legal obligations under the Data Protection Act 1998 in relation to the protection of personal data that it holds about or concerning any individual. All employees, Barnet Councillors, staff members or partner organisations (suppliers and contractors) who have been permitted access by the Council to personal data must familiarise themselves fully with the policy and ensure that its terms are applied fully in relation to the handling or “processing” of personal data.

This policy concerns personal data held by the Council in relation to any person.

Data protection is monitored by the Information Commissioner's Office, an independent official body. The Information Commissioner is responsible for administering the provisions of the Data Protection Act 1998 (“the Act”) and has powers to take legal action against businesses or individuals found to be acting unlawfully. An employee may make themselves individually liable to legal action by the Information Commissioner and/or by any individual whose information they have disclosed in breach of data protection legislation and who suffers loss as a result.

This policy is designed to protect the Council, staff, clients, partner organisations and members of the public by preventing such breaches from happening. The policy seeks to ensure that personal data processed by or on behalf of the Council is dealt with in full compliance with the Act.

A copy of the Act can be located on the Office of Public Sector Information website [www.opsi.gov.uk](http://www.opsi.gov.uk)

## 2. Policy Statement

The Council is committed to compliance with its legal obligations and with good practice guidance. As part of normal business practice and in order to effectively deliver services, from time to time the Council needs to collect personal data. The Council always tries to ensure the information collected is accurate and isn't an invasion of anyone's privacy.

The Council is aware that personal information must be collected, recorded, stored and used in the correct manner and in accordance with the Act.

Employees who are involved with the handling of personal data will receive appropriate training during their employment and they will receive continued support and guidance from the Data Protection Officer.

The Council will ensure that it treats personal information lawfully and correctly and adhere to the Principles of Data Protection as defined in the Act.

### 3. Data Protection Principles

The Act contains eight Principles which must be complied with when processing personal data: -

- **First** - 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 (of the Act) is met, and  
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (of the Act) is also met.
- **Second** - 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.
- **Third** - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Fourth** - Personal data shall be accurate and, where necessary, kept up to date.
- **Fifth** - Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- **Sixth** - Personal data shall be processed in accordance with the rights of data subjects under the Act.
- **Seventh** - 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.
- **Eighth** - 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.

### 4. Subject Access Requests

Under the Act individuals (“Data Subjects”) have the legal right, subject to some exemptions, to see information about themselves that is held by the Council. The request (“Subject Access Request”) has to be made by the Data Subject in writing and may be subject to a £10 (there is no charge for students, pensioners, staff, benefit claimants and those on Income Support).

Anyone making a Subject Access Request will have to pay a fee (if charged) for every request, so they should ensure that they specify all the information

they need in their first letter, otherwise they may have to pay another fee to get information they have asked for on a different occasion.

The Council may need them to supply further information to satisfy itself as to their identity. E.g. a copy of their passport/birth certificate or bank/utility bill (showing full address).

Responses to any subject access requests will be prompt and in any event within the statutory 40 calendar days from when both identification confirmation and payment have been received from the Data Subject.

Personal information may be withheld from disclosure to the extent that if it falls under any of the exemptions described in the Act. A copy of the Act can be located on the Office of Public Sector Information website [www.opsi.gov.uk](http://www.opsi.gov.uk).

## 5. Exemptions

The Council is exempt from its duty to disclose in certain circumstances and can withhold information under the Act. If anyone is denied information on the grounds of an exemption they will be notified of the exemption that applies. More information can be found on the ICO website ([www.ico.gov.uk](http://www.ico.gov.uk)) under 'Exempt information'.

## 6. Responsibilities of Staff

The Council will use all reasonable endeavours to ensure, through appropriate training and management, that officers' responsibilities under the Act are adhered to. In addition to this: -

- Staff have a personal and contractual responsibility to ensure that their processing of personal data they process complies with the Data Protection Principles detailed in (3) above.
- Managers must ensure that their area of operation complies with the Act and their use of personal data is registered. Managers must ensure that staff are aware of the relevant policies and procedures.
- Managers must ensure that personal data held in their service areas are only processed for one or more of the purposes described in the Council's entry on the Data Protection Register
- Data sharing must be subject to a written protocol/agreement setting out the powers that permit the exercise, its scope and controls.
- Data transfer must only be undertaken following the guidelines outlined in the Council's Data Transfer Security Policy.
- Processes for handling personal information must be regularly assessed.
- All employees must take steps to ensure that all personal data is kept secure at all times.

- All employees must be made fully aware of this policy and of their duties and responsibilities under the Act.
- Any member of staff knowingly or recklessly breaching this Data Protection Policy and/or legislation may be subject to the Council's disciplinary procedures.

## 7. The Role of the Information Commissioner

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

- conduct assessments to check organisations are complying with the Act;
- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified 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 of 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.

## 8. Definitions

Some key terms used in the data protection legislation have been broadly defined below:-

### **Data**

Information which is: -

- processed by equipment operating automatically (or stored with the intention that it will be processed automatically) or is recorded as part of a relevant filing system (including manual data) or is an accessible public record;
- recorded as part of a relevant filing system (including manual data);
- an accessible public record; or
- held by a public authority

Included are e-mails (archived, backed-up, deleted or capable of recovery), document imaging systems, video surveillance equipment, manual files kept in a structured filing system so that the criteria relates to individuals (e.g. paper files, card indexes) and all other information recorded by a public authority.

### **Data Controller**

The organisation ultimately responsible for the processing of personal data and who controls and benefits from such processing. In our case, this is the Council.

### **Data Subject**

The individual about whom the personal data relates.

### **Personal Data**

Data which relates to a living individual who can be identified from those data or from those data and other information which is the possession of, or is likely to come into the possession of, the data controller. Personal data relating to employees is included.

### **Processing**

Obtaining, recording, or holding the data or carrying out any operation or set of operations on the data, including: organising, adapting, altering, retrieving, consulting, using, transmitting, disseminating, making available, aligning, combining, blocking erasing or destroying the data.

### **Sensitive Personal Data**

Personal data about the racial or ethnic origin of the data subject, his political opinions, religious or similar beliefs, trade union membership, physical/mental condition, sexual life, commission (or allegations) of an offence or proceedings relating to an offence.

## **9. Contact Information**

Further advice and guidance is available from the Information Governance Officer.

Members of the public who wish to access their personal data should write to the Information Governance Team at the address below.

Address: Governance Officer, London Borough of Barnet  
North London Business Park, Oakleigh Road South  
London  
N11 1NP

Tel No: 020-8359-2029

E-mail: [data.protection@barnet.gov.uk](mailto:data.protection@barnet.gov.uk)

Website: [www.barnet.gov.uk/data-protection-act](http://www.barnet.gov.uk/data-protection-act)