

# **Data Protection Policy**

## **Introduction**

West London Waste Authority is fully committed to compliance with the requirements of the Data Protection Act 1998 (the “Act”), which came into force on 1 March 2000. The Authority will therefore follow procedures that aim to ensure that all employees, members, contractors, agents, consultants, partners or other servants of the Authority who have access to any personal data held by or on behalf of the Authority, are fully aware of and abide by their duties and responsibilities under the Act.

## **Statement of policy**

In order to operate efficiently, the Authority has to collect and use information about people with whom it works (i.e. its employees and members). The Authority does not collect or use information about any other people. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

The Authority regards the fair and lawful treatment of personal information as very important to its successful operations and to maintaining confidence between the Authority and those with whom it carries out business. The Authority will ensure that it treats personal information fairly and lawfully.

To this end the Authority will comply with the Data Protection Principles set out in Part 1 of Schedule 1 of the Act. Any breach of this Data Protection Policy or the Act will automatically be considered a breach of discipline and existing Authority disciplinary proceedings may apply.

## **The Principles of Data Protection**

The Act stipulates that anyone processing personal data (the “data processor”) must comply with Eight Principles of good practice. These Data Protection Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. 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. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. 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. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection

## **Personal Data and Sensitive Personal Data**

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from:

- That data; includes name, address, telephone number, id number, date of birth etc
- That data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

## **Handling of personal/sensitive personal information**

The Authority will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information;
- Specify the purpose for which the Authority will use personal information;
- Collect and process personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure that the personal information it processes is accurate and up to date;
- Apply checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held ("data subjects") can be fully exercised under the Act. These include:
  - The right to be informed that processing is being undertaken;
  - The right of access to one's personal information within 40 days;
  - The right to prevent processing in certain circumstances;
  - The right to correct, rectify, block, have noted any information that the data subject regards as incorrect or erase information regarded as wrong information.

In addition, the Authority will ensure that:

- There is someone with specific responsibility for data protection in the Authority;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information will be regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out in accordance with the Data Protection Principles. Any disclosure of personal data will be in compliance with approved procedures.

### **Management Responsibilities**

All managers and staff within the Authority will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

### **Contractors' Responsibilities**

All contractors, consultants, partners or other servants or agents of the Authority must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Authority, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Authority and that individual, company, partner or firm;
- Allow data protection audits by the Authority of data held on its behalf (if requested);
- Indemnify the Authority against any prosecutions, claims, proceedings, actions or payments of compensation or damages.

All contractors who process personal information supplied by the Authority will be required to confirm that they will abide by the requirements of the Act with regard to personal information supplied by the Authority.

## **Implementation**

The Head of Finance will be responsible for data protection including:

- Provision of data protection training for relevant staff.
- Carrying out appropriate checks to ensure compliance with the Act.
- Provision of professional support, updates and advice to officers and staff on data protection and related matters
- Notification to the Information Commissioner

## **Notification to the Information Commissioner**

The Information Commissioner maintains a public register of data controllers. West London Waste Authority is registered as such -- Registration Number **Z6963439** accessible at

<https://ico.org.uk/ESDWebPages/Search?EC=3&fieldname=West%20LondonWaste%20Authority>

The Act requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. To this end the Head of Finance will review Data Protection issues as they arise and, prior to notification to the Information Commissioner.

## **Review of Data Protection Policy**

The policy will be reviewed on any material change to the business or legislation and in light of any notifications to the Information Commissioner.

## **Glossary of Technical Terms under the Data Protection Act 1998:**

“data” means information which-----

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined;

“data controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

“data processor” in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

“data protection principles” mean:

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, and

(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 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.

“data subject” means an individual who is the subject of personal data;

“personal data” means data which relate to a living individual who can be identified-----

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come

into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

“processing”, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-----

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

“relevant filing system” means 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.

“sensitive personal data” means personal data consisting of information as to-----

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings