West London Waste

Treating waste as a valuable resource

Data Protection Policy

Minor amendments approved by the Clerk in January 2022.

Introduction

West London Waste Authority is fully committed to compliance with the requirements of the Data Protection Act 2018 (the ‘‘Act’’), and the UK GDPR (“the data protection legislation”). 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) and customers. 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, in video or recorded by anyother 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 3, Chapter 2 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 six Data Protection 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 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.

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 special category 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.

Special category data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data;
- Physical or mental health or condition;
- Sexual life;
- Sexual orientation.

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 one calendar month;
    -The right to rectify any inaccurate or incomplete personal data;
    -The right to request deletion or removal of personal data;
    -The right to block or restrict processing of personal data;
    -The right not to be subject to automated decision-making.

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 and Employee 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.

Both individuals and organisations can be held liable for breaches of the data protection legislation and subject to penalties.

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.

National Fraud Initiative (NFI)

The Authority is required [by law] to protect the public funds it administers. It may share information provided to it with other bodies responsible for; auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect fraud.

The Cabinet Office is responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise, including payroll.

The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the data protection legislation.

Implementation

The Finance Director 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/Entry/Z6963439

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 Finance Director 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.

Procedures

The Authority processes a very limited amount of personal data for a very limited number of reasons. This includes personal data for HR/payroll, booking systems and engagement activities.

A data register will be maintained identifying key information including the nature of personal data, the processing, location of privacy notice and consent records and the responsible managers.

Responsible managers will ensure suitable procedures are in place including processes for data security, data management and data rights requests. The Finance Director will ensure regular audit/assurance of procedures and appropriate reporting.