Merseyside Waste Disposal Authority (MWDA)

Data Protection Policy

1) Statement of Commitment

2) Policy Objectives

3) Meeting Our Policy Objectives

4) Data Security

5) Data Access and Data Sharing

6) Compliance with this Policy

1.0. Statement of Commitment

(i) We understand the importance of ensuring that personal data, including sensitive personal data is always treated lawfully and appropriately and that the rights of individuals are upheld.

(ii) We are required to collect, use and hold personal data about individuals. Data is required for the purposes of carrying out our statutory obligations, delivering services and meeting the needs of individuals that we deal with.

(iii) This includes current, past and prospective employees, service users, members of the public, Members of the Authority, our business partners and other local authorities or public bodies.

2.0. Policy Objectives

(i) In order to comply with the requirements of the Data Protection Act 2018 (General Data Protection Regulation (GDPR) we will ensure that:

a. Any personal data will be collected, used and held, lawfully and appropriately.
b. Regular data sharing with external partners and other relevant agencies will be subject to data sharing agreements.
c. Partnerships will only be entered into where there is a clear statutory power enabling the Authority to participate.
d. External agencies contracted to undertake any data processing on behalf of the Authority will be required to demonstrate compliance with the Data Protection Act 2018 (General Data Protection Regulation (GDPR) and satisfy the Authority that it has the necessary technical and organisational measures in place to protect personal data.
e. The Authority has a range of policies and procedures in place which are regularly reviewed and updated to ensure staff understand their responsibilities towards protecting personal data.
f. Training needs are identified and provided to ensure that those handling personal data are trained appropriately.
g. There is an appointed officer (Data Protection Officer [DPO]) within the organisation who has specific responsibility and knowledge about data protection compliance, covering all aspects within the scope of this Policy and who is a point of contact for all queries.
h. Data subjects rights can be fully exercised.

i. Subject Access Requests from individuals are dealt with promptly and courteously.
j. Any new projects being implemented that involve personal data will undergo a Pre-Data Privacy Impact Assessment.
k. We will regularly review and update this Policy, procedures and guidance for Authority employees and Members.
l. We are required by law to share or make available some of the personal data we collect and hold. This information may be shared for a number of reasons including to:

- Safeguard public funds
- For the prevention and detection of fraud
- For the prevention and detection of crime.

For further details on this please read our Corporate Privacy Notice. http://www.merseysidewda.gov.uk/wp-content/uploads/2018/11/MWDA-CORPORATE-PRIVACY-NOTICE-2018-FINAL.pdf

(ii) The Authority is fully committed to complying with the requirements of the Data Protection Act 2018 (General Data Protection Regulation (GDPR) and is registered as a data controller with the Information Commissioner's Office (ICO). Our registration number is Z8317644. The register can be viewed at: www.ico.org.uk

3.0. Meeting our Policy's Objectives

(i) In order to meet the objectives we need to ensure that they are always considered and that appropriate controls and procedures are in place to ensure compliance. These will include:

a. When we collect personal data we will ensure that where required, we make individuals aware that their information is being collected.*
b. We will always specify the purpose for collecting the data specified.*
c. We will always specify if the data it will be shared with any third parties.*
d. We will always specify how long we will keep the data.*

(points a – d will be delivered through the use of the Authority's two Privacy Notices.

e. When reviewing documents and forms, we will always consider whether any personal data collection or processing is needed.

f. No new purpose for processing data will take place until advice has been received from the MWDA DPO, and data subjects have been notified of the relevant new purpose.
g. We will ensure that when that customers are utilising services via the telephone that staff are fully aware of the guidelines when collecting, confirming or supplying personal information as part of those processes
h. We will ensure that good document handling and processing practices are adhered to within the Authority's main office and administrative process to ensure personal data is secure.
i. The Authority will work with its two main waste contractors - Veolia Merseyside and Halton and SUEZ UK and Merseyside Energy Recovery Limited to ensure that all personal data collected as part of the operational activities fall with existing contractual processes or that a data sharing agreement is in place.

4.0. Data Security

(i) Authority employees and Members must report any suspected data breaches to the Data Protection Officer for investigation and where necessary the Data Protection Officer will notify the Information Commissioner's Office.

(ii) A data breach is when personal data is lost, stolen, mistakenly shared with another party or partially or completely destroyed.

(iii) If a data breach occurs :

a. Please inform the Data Protection Officer as soon as you become aware of a data breach occurring
b. It is a requirement to report a personal data breach to the ICO within 72 hours, unless the Authority can demonstrate it's unlikely to result in a risk to individual's rights and freedoms.
c. Information that needs to be provided in the event of a personal data breach:

- How has the data been lost?
- How many people could be affected and how many records?
- Is it staff or customer data that has been affected?
- When was the data breach noticed?
- What type of data has been breached?
- Is there any sensitive information?
- If the data was taken or lost via a device please identify the device and what type of security on encryption it included
- If the data was taken or lost as a hard copy please identify the document.

(iv) Authority employees and Members must always use appropriate levels of security to store or share personal data both within the office environment, and on any mobile or remote devices they might utilise.

(v) Personal data is also included in a range of hard copy documentation. In the most part this information will be retained securely within the office environment, but the Authority recognises that there are occasions and systems that may require this information to be utilised in other locations and this includes the Authority's Business Continuity Plan

a. A Business Continuity Plan: A hard (paper) copy of the Plan is issued to the Chief Executive, Directors, Assistant Directors and Managers and some other key personnel. As part of the issue of this information it is reinforced that the document does contain personal information of staff and should be kept securely by the individual. Any loss of the document must be reported immediately

(vi) Guidance and training on the security of using Authority IT systems, hardware and mobile devices is provided to employees as part of the Authority's Email and Internet Policy.

(vii) When new projects involving personal data are being developed, Pre -Privacy Impact Assessments will be carried out by the Project Manager and reviewed by the Data Protection Officer in order to assess any privacy risks.

(viii) An Document and Data Retention Document will be maintained by the Data Protection Officer identifying:

a. All personal data held
b. Where it is held
c. How it is processed
d. What teams have access to it
e. Who has overall responsibility for the data?
f. A Data Destruction record for all personal data that has been destroyed or deleted.

(ix) Personal data will not be shared with a third party organisation without a valid business reason and where required we will notify individuals that the sharing will take place in the form of a privacy notice. If any new purposes for the data sharing are to take place, we will seek consent from the individuals concerned.

(x) When personal data is shared regularly with a third party, a Data Sharing Agreement must be implemented. Any data sharing will also take into consideration:

a. Any statutory basis of the proposed information sharing
b. Whether the sharing is justified

c. How to ensure the security of the information being shared.

5.0. Data Access and Data Sharing

(i) Our employees and Members will have access to personal data only where it is required in order to fulfil their role.

(ii) All data subjects have a right of access to their own personal data; employees will be made aware of and will provide advice to data subjects about how to request or access their personal data held by us. More information is available on our Personal Data Requests page http://www.merseysidewda.gov.uk/contact-us/personal-data-requests/

(iii) Our employees and Members are aware of what to do when requests for information are made under the Data Protection Act 2018 (General Data Protection Regulation (GDPR).

(iv) Our employees and Members are made aware that in the event of a Subject Access Request (by an individual or being received by us, their emails may be searched and relevant content disclosed.

(v) Data Request Record

(vi) The Authority's Privacy Notices include a contact address for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how we are processing their data, or about the handling of a Subject Access Request.

(vii) A Subject Access Request will be acknowledged to the data subject within 24 hours, with the final response and disclosure of information (subject to exemptions) within 30 calendar days.

(viii) A data subject's personal data will not be disclosed to them until their identity has been verified.

(ix) Third party personal data will not be released by us when responding to a Subject Access Request (unless consent is obtained, it is required to be released by law, or it is deemed reasonable to release).

6.0. Compliance with this Policy

(i) This Policy applies to all our employees, Authority Members and all people or organisations acting on behalf of the Authority.

(ii) The Authority's Chief Executive, Directors, Assistant Directors and Managers shall ensure compliance with this Policy appropriate to the personal data activities within their remit and manages within their section, project or team.

(iii) If any Authority employee, or Member or persons acting on our behalf are found to knowingly or recklessly breach the Authority's Data Protection Policy appropriate disciplinary and/or legal action will be taken.

(iv) The Authority has a designated Data Protection Officer with data protection knowledge in all service areas.

(v) Implementation of this Policy will be led by the Data Protection Officer. Any questions or concerns about this Policy should be directed to the Data Protection Officer.

Contact details:

MWDA Data Protection Officer, Tel: 0151 255 2527

Email: enquiries@merseysidewda.gov.uk