DATA PROTECTION POLICY

1. General Policy Statement

In order to operate efficiently, JWS Waste and Recycling Services Limited (JWS) are required to obtain and process relevant personal data about individuals it works alongside. This allows us to carry out our business as intended and provide planned services to our customers. Individuals we are required to obtain data from include, but are not limited to; current, past and prospective employees, agency staff, customers, suppliers and contractors. No matter how the information is obtained, personal data will be processed at JWS in accordance with this Policy to ensure compliance with the General Data Protection Regulations 2016 (GDPR) and our own internal procedures.

JWS regard the lawful and correct treatment of personal information as integral to the achievement of our objectives, to the success of our operations, and to maintaining confidence between ourselves and those we deal with. We therefore ensure that our organisation treats personal information lawfully, correctly and in accordance with the Data Protection Principles outlined in Article 5 of the GDPR.

This Data Protection Policy has been written to provide the frame work through which effective data management is achieved at JWS. It outlines the steps JWS have implemented and the cooperation we expect from those working alongside us to ensure all round compliance. The purpose of the Policy is to inform JWS staff and those working with us of their duties under the GDPR and set out the standards expected by JWS in relation to the processing of personal data.

2. Principles

JWS shall, so far as is reasonably practicable, will comply with the Data Protection Principles outlined in the GDPR, to ensure all data is:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
d) Accurate and, where necessary, kept up to date; with every reasonable step taken to ensure that inaccurate personal data are erased or rectified without delay.
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

JWS management have implemented a number of measures to ensure compliance with the above principles, some of which are summarised below:

- Adopting and implementing this Policy.
- Taking a ‘data protection by design and default’ approach.
- Ensuring organisations we share personal data with are compliant with our Data Protection Policy and only process data in accordance with the written instructions provided to them by JWS.
- Maintaining documented records of our processing activities and our lawful basis for doing so.
- Implementing appropriate technical and organisational security measures.
- Recording and, where necessary, reporting personal data breaches.

- Training staff to understand their role in data protection within the organisation.
- Making data subjects aware of our Privacy Policy when collecting personal data.

3. Roles and Responsibilities

The Directors' of JWS have overall responsibility for compliance with the GDPR and associated guidance. However, individual employees are responsible for the correct and proper use of the data they process.

JWS employees who handle personal data are expected to:
- Familiarise themselves with and abide by the Data Protection Principles outlined above.
- Read and understand this Policy document.
- Understand how to conform with the standards expected of them in relation to data protection.
- Understand what is meant by 'special categories of personal data' and know how to handle such data.
- Attend training to ensure their understanding.

4. Data Protection Controller

JWS are not required to appoint a Data Protection Controller as we do not fall under the requirements outlined in the GDPR. We do however have a dedicated team, with relevant training and experience, on hand to assist staff comply to internal procedure, handled data subject enquiries and ensure overall compliance with the GDPR.

5. Processing Personal Data

Personal data is defined as any information relating to an identifiable person who can be directly or indirectly, identified, in particular by reference to an identifier. Processing of personal data is widely defined to include acquisition, holding, amending, disclosure and deletion of data. Personal data must only be processed for the purpose(s) for which it was obtained or for a similar purpose.

JWS will ensure the lawful basis is identified and recorded before processing any personal data. The lawful basis for processing data, as identified in the GDPR, are as follows:

a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
d) Vital interests: the processing is necessary to protect someone's life.
e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6. Sensitive Personal Data

The GDPR, Article 9, refers to sensitive personal data as "special categories of personal data", revealing racial or ethnic origin, political opinion, religious beliefs and health as examples. Where sensitive data is to be obtained explicit consent will be obtained from the subject.

7. Right of Access

JWS provides the following rights for all individuals for which we hold data:
- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object to processing
- Rights in relation to automated decision making and profiling.

In line with the GDPR data subjects have the right of access to information held by JWS (Subject Access Request). Subjects wishing to access their personal data must contact the Compliance Department who will review the details and:

- Charge for, or refuse only where the request is manifestly unfounded or excessive.
- If refusing, inform the individual why without undue delay and at the latest within one month, also informing them that they have a right to complain to the supervisory authority and to a judicial remedy.
- If responding, do so within one month.

All subject Access Requests received by JWS will be logged and a record of the information requested and provided maintained.

8. Exemptions

Certain data is exempt from the provisions of the GDPR, under Article 23. As an example, this includes:

- National and public security and the prevention or detection of crime
- The assessment and any tax or duty

9. Accuracy

JWS will endeavour to ensure that all personal data held in relation to data subjects is accurate. Individuals are required to inform JWS of any changes to information held about them. Personal data will be reviewed periodically to check that it remains accurate and up to date and to determine if retention or secure destruction is necessary.

JWS have a dedicated team to monitor and over see data protection procedures at JWS to ensure ongoing compliance. In addition the team will endeavour to audit the procedures in full on an annual basis to help identify any improvements that can be implemented.

10. Data Security

JWS will take appropriate technical and organisational steps to ensure the security of all personal data held. JWS staff will be made aware of this Policy and their duties held under the GDPR. Employees are required to respect personal data and the privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or authorised processing or disclosure of personal data and against accidental loss of or damage to the data. JWS will monitor their Data Protection Policy and procedures, conducting regular internal audits. Breaches identified will be reported to the relevant supervisory authorities where necessary and will be investigated fully to determine the cause and identify any corrective and preventative measures necessary.

Unlawful obtaining or disclosure of personal data by JWS employees or other breathes of the GDPR will be treated seriously and may lead to disciplinary action. Where a data breach occurs or is suspected a non-conformance will be raised immediately and passed to the Compliance Department for review.

If an individual believes that JWS have not complied with this Policy or acted in accordance with the GDPR they should inform JWS in writing. Individuals also have the right to inform the Data Protection Commissioner if they believe their data has not been processed in accordance with the regulatory requirements.

11. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. A DPIA is carried out were processing data is likely to result in a high risk to individuals, which is assessed by considering both the likelihood and the severity of any impact on individuals.

12. External Party Processors

JWS do not pass personal data to outside organisations unless defined by the identified and recorded lawful basis and required for completion of the requested service.

Where information is passed outside of the organisation JWS will endeavour to ensure that all external processors are compliant with the GDPR and will request they adhere to JWS Policies and Terms in relation to data processing. External parties must protect the rights of data subjects and duly observe all its obligations under the GDPR. They must only process data as per the documented instructions provided by JWS and for the purpose the data is provided. Sub-processed is not permitted without permission from JWS and the external party must take all necessary protective measures to ensure the security of the data. Breaches, suspected breaches, or concerns must be report to JWS within 24 hours and a full investigation undertaken.

13. Retention and Destruction

JWS may retain data for different periods of time for different purposes as required. Individual departments have incorporated procedures for retention into their processes and this is recorded on our retention log.

When data held in accordance with this Policy is destroyed, it will be destroyed securely in line with best practice at the time of destruction. Data will not be held for longer than is necessary, the company QEHS management system should be consulted for guidance on what is necessary for each kind of data.

14. CCTV

JWS own and operate a CCTV network on site for the purpose of crime prevention and detection. It may also be used for health and safety, monitoring working activities on site and investigating accidents or incidents. Where a data subject can be identified on CCTV footage the images will be processed as personal data.

15. Contact

For enquires regarding this Data Protection Policy and for formal access requests please write to:

Compliance Department
JWS Waste and Recycling Services Limited
Westport House
35 Frederick Road
Salford
M6 6LD

complaince@jwswaste.co.uk

This Policy will be reviewed by a Company Director on an annual basis or sooner if necessary following a change in internal procedures or legislation.

PETER ANDREW
MANAGING DIRECTOR