Privacy Policy

1. Policy Statement

Every day MSO will receive, use and store personal information about our customers, suppliers and colleagues. It is important that this information is handled lawfully and appropriately in line with the requirements of the [Data Protection Act 1998] and the General Data Protection Regulations GDPR.

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy sets out the basis on which we will process any personal data we collect or process.
This policy does not form part of any employee's contract of employment and may be amended at any time.
The Data Protection Officer is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer or reported in line with the organisation's Whistleblowing Policy or Grievance Policy.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.

e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and 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.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

5. Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

6. Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

7. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

9. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed.
b. Request access to any data held about them by a data controller (see also *Clause 15 Subject Access Requests*).
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority.
e. Data portability.
f. Object to processing including for direct marketing.
g. Not be subject to automated decision making including profiling in certain circumstances.

10. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on MSO's central computer system instead of individual PCs.

Security procedures include:

a. **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
b. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. **Data minimisation.**
d. **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
e. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

11. Disclosure and Sharing of Personal Data

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

12. Subject Access Requests

Individuals must make a formal request for information we hold about them. Employees who receive a request should forward it to the Data Protection Officer immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:
We will check the caller's identity to make sure that information is only given to a person who is entitled to it. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible.

Our employees will refer a request to their line manager or the Data Protection Officer for assistance in difficult situations.

13. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.