Data Protection Policy

1. STEELITE INTERNATIONAL POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our employees, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that we may be required to handle include information about current, past and prospective employees. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in The General Data Protection Regulation (GDPR) and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the GDPR.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings, genetic data and biometric data where processed to uniquely identify a person (for example a photo in an electronic passport). Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the principles of data protection. These provide that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals.
(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is 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 is processed; personal data may be stored for longer periods insofar as the personal data will be processed 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.

4.2 The data controller is responsible for and must be able to demonstrate compliance with these principles of data protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The GDPR is 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 data subject.

5.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

6.1 In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources.

6.2 We will only process personal data for specific purposes or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will inform them about their rights under the GDPR (please refer to the Steelite International Limited Privacy Notice) including:

(a) The purpose or purposes for which we intend to process that personal data and the legal basis for the processing.
(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.
(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data including the right to object to processing.
(d) The right of subject access.
(e) The right to be forgotten.
(f) The right to withdraw consent, where processing is based on consent.
(g) The right to rectification if data is inaccurate or incomplete.
(h) Rights related to automated decision making and profiling.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information, if necessary, as soon as possible thereafter.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

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

8.2 The specific purposes for which we will need to collect personal data about a data subject includes:

(a) Allocating work.
(b) Providing salary and benefits in accordance with the terms and conditions of employment or legislation and reviewing salary and benefits.
(c) Managing conduct, performance or absence.
(d) Processing information about an employee's absence or medical information in order to assess eligibility for sick pay or other insurance, health or pension benefits, to determine fitness for work generally or at a specific time or for a specific job or duties, making decisions about alternative duties or alternative jobs or adjustments necessary where the employee may not be fit for existing duties or jobs and making decisions about employment or continued employment.
(e) Disciplinary investigations, disciplinary hearings and making and recording disciplinary decisions and appeals in relation to those decisions.
(f) Investigating and deciding on grievances which an employee may raise or are indeed raised by other personnel regarding an employee or where the employee is a witness.
(g) Carrying out reorganisations or redundancies including redundancy consultation, selection, dealing with any appeals and searching for and finding alternative employment.
(h) Consultations and negotiations with trade unions, elected employee representatives, work councils or other collective consultation bodies.
(i) Making decisions regarding promotion or transfer.
(j) Carrying out formal and informal appraisals or reviews, or any other training or development requirements.
(k) Compliance with legislation (for example Statutory Sick Pay rules, Working Time Regulations, Gender Pay Gap Regulations, Minimum Pay Regulations, PAYE arrangement).
(l) Monitoring of equality of opportunity with regard to gender, marital status, race, ethnic origin, colour, nationality, national origin, disability, sexual orientation, religion or age.
(m) Making the skills and expertise of the data subject known within the organisation.
(n) Disclosure where reasonably necessary for the purposes of publicity material or obtaining business from actual or potential customers, annual reports or similar business documentation.
(o) Disclosure of information where necessary, for contact purposes, internally and externally with customers, suppliers and other third parties for the purposes of ensuring the smooth conduct of the business of the Company.
(p) Maintaining records necessary to manage the employment relationship.
(q) Disclosure of information where necessary to third parties in relation to information requested from Government bodies and professional institutions (for example taxation, child support, police, mortgage and pension requests).

9. ACCURATE DATA

9.1 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.

10. TIMELY PROCESSING

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

11. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

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

(a) Request access to any data held about them by a data controller (see also clause 15).
(b) Object to processing, including in particular to prevent the processing of their data for direct-marketing purposes.
(c) Ask to have inaccurate data amended (see also clause 9).
(d) Request the deletion or removal of personal data where there is no compelling reason for its continued processing.
(e) Prevent processing that is likely to cause damage or distress to themselves or anyone else.
(f) Obtain and reuse their personal data for their own purposes (where that right applies)

12. DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. If there is a data security breach which will result in a risk to the data subject we will report that breach to the regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he/she agrees to comply with those procedures and policies, or if he/she puts in place adequate measures him/herself.

12.3 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 our central computer system instead of individual PCs.

12.4 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) Methods of disposal. Paper documents should be shredded or disposed of in lockable confidential waste bins. Digital storage devices should be physically destroyed when they are no longer required.

(d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from or lock their PC when it is left unattended.

13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

13.1 We will only transfer any personal data we hold to a country outside the European Economic Area ("EEA") where the conditions of transfer provided for in the GDPR apply.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

14.1 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.

14.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.4 We may also share personal data we hold with selected third parties.

15. DEALING WITH SUBJECT ACCESS REQUESTS

15.1 Data subjects must make a formal request for information we hold about them. This must be made in writing.

15.2 When receiving telephone enquiries, we will not disclose personal data we hold on our systems. We will ask the caller to put their formal request in writing.

15.3 Employees should not be bullied into disclosing personal information.

16. CHANGES TO THIS POLICY

16.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes.

Last updated: Wednesday 18th April 2018.