Data Protection Policy

1. Policy statement and scope of policy

1.1 SML Group Ltd ("we", "our", "us", "the Company") is committed to ensuring that the use of personal data throughout the Company is in accordance with legal requirements and that the integrity and protection of data are maintained at all times.

1.2 All individuals have rights in relation to the handling of their personal data. During the course of its activities, the Company will collect, store and process personal data and the Company recognises the need to treat all such personal data in an appropriate and lawful manner.

1.3 Employees, workers, officers and consultants of the Company also have obligations in relation to the processing of personal data whilst working for or on behalf of the Company and are expected to comply with this Policy.

1.4 This policy sets out how the Company will handle the personal data of its customers, suppliers, officers, employees, workers, consultants, agency workers, job applicants, work placement students, visitors, targets, contacts and other third parties. This policy sets out the Company's rules on data protection and the legal conditions that must be satisfied in relation to the processing of personal data.

1.5 In this policy, when we refer to "you" or "your" we are referring to employees, workers, officers and consultants employed or engaged by the Company.

1.6 This policy seeks to comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) and any other regulations that govern the processing of personal data from time to time ("the Data Protection Laws").

1.7 This policy does not form part of an employee's contract of employment with the Company and it may be amended at any time. Any breach of this policy by an officer, employee, worker, agency worker or consultant will be taken seriously and may result in disciplinary action in relation to employees and other action in relation to non-employees. In some instances, serious breaches of this policy may be considered to be an act of gross misconduct which could result in the immediate termination of employment, or, as is the case, the immediate termination of any consultancy or engagement.

2. Definition of data protection terms used in this policy

2.1 Automated Decision Making (ADM) means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

2.2 Automated Processing means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

2.3 Consent means agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data or Special categories of Personal Data relating to them.

2.4 Criminal Offence Data means any Personal Data which relates to an individual's criminal convictions and offences.

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

2.6 Data Controller means the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with GDPR. The Company is the Data Controller of all Personal Data relating to our officers, employees, workers, consultants, job applicants, work placement students, customers, targets, contacts, visitors and suppliers and of others which the Company uses in our business.

2.7 Data Privacy Impact Assessment means assessments used to identify and reduce risks of a data processing activity.

2.8 Data Subjects for the purpose of this policy include all living 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 Data.

2.9 Explicit Consent means Consent which requires a very clear and specific statement (that is, not just action).

2.10 Personal Data means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that Data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous Data or Data that has had the identity of a Data Subject permanently removed. Personal Data can be factual or an opinion about a Data Subject's actions or behaviour. Examples of Personal Data relating to an identified or identifiable individual includes, but is not limited to, information revealing their name, address, email address, identification number, location data, online identifiers, and/or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity

2.11 Personal Data Breach means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

2.12 Privacy Notices means separate notices setting out prescribed information that must be provided to Data Subjects when the Company collects Personal Data relating to them or when the purpose for which Personal Data is Processed changes.

2.13 Processing or Process is any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing includes transferring Personal Data to third parties.

2.14 Pseudonymisation or Pseudonymised means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the Data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

2.15 Special categories of Personal Data means Personal Data which relates to an individual's health, sex life, sexual orientation, racial or ethnic origin, political opinion, religion or philosophical belief, and trade union membership. It also includes genetic and biometric data (where used for identification purposes).

3. Data Manager

3.1 The Company has appointed a Data Manager who is responsible for ensuring the Company's compliance with this policy and the Data Protection Laws. The Company's Data Manager is Simon Corbett, Financial Director whose contact details are: email: simon.corbett@sml-group.co.uk Tel: 0116 4974551 and address: SML Group Ltd, 8 Garden Street, Thurmaston, Leicester, LE4 8DS

4. Personal Data protection principles

4.1 The Company adheres to the principles relating to Processing of Personal Data set out in the Data Protection Laws which require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

4.1.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation);

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

4.1.4 Accurate and where necessary kept up to date (Accuracy);

4.1.5 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Data is Processed (Storage Limitation); and

4.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

4.2 The Company is responsible for and will seek to demonstrate compliance with the above principles (Accountability).

5 Lawfulness, Fairness and Transparency

5.1 The Company will only collect, Process and share Personal Data fairly and lawfully and for specified purposes.

5.2 The Data Protection Laws set out the specified purposes ("Permitted Purposes") for which Personal Data may be Processed. The Company relies on one or more of the following Permitted Purposes when Processing Personal Data:

5.2.1 The Data Subject has given his/her Consent;

5.2.2 The Processing is necessary for the performance of a contract with the Data Subject;

5.2.3 The Processing is necessary to comply with the Company's legal obligations;

5.2.4 The Processing is necessary in order to protect the vital interests of the Data Subject; and/or

5.2.5 The Processing is necessary to pursue the Company's legitimate interests (or the legitimate interests of a third party (i.e. a benefits provider or pensions adviser)) where those legitimate interests are not overridden by the interests or fundamental rights and freedoms of the Data Subject.

5.3 In addition to the Permitted Purposes set out in paragraph 5.2 above, the Data Protection Laws set out further additional specified purposes ("Additional Purposes") that the Company must be able to demonstrate if it wishes to Process Special categories of Personal Data. The Company will seek to rely on one or more of the following Additional Purposes when Processing Special categories of Personal Data:

5.3.1 The Data Subject has given his/her Explicit Consent;

5.3.2 The Processing is necessary for carrying out the Company's rights and obligations under employment laws, social security laws or social protection laws;

5.3.3 The Processing is necessary to protect the vital interests of the Data Subject or those of another person and where the Data Subject is not physically or legally capable of giving Consent;

5.3.4 The Data Subject has already made the Special categories of Personal Data public;

5.3.5 The Processing is necessary for the establishment, exercise or defence of legal claims;

5.3.6 The Processing is necessary for the purposes of occupational medicine or for the assessment of the working capacity of an employee, worker, officer or consultant;

5.3.7 The Processing is necessary for reasons of substantial public interest, on the basis of UK/EU law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject; and/or

5.3.8 The Processing is necessary for archiving purposes in the public interest or for statistical purposes based on UK/EU law which shall be proportionate to the aim pursued, respect the essence of data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject. Those safeguards shall ensure that technical and organisational measures are in place in particular to ensure data minimisation and may include Pseudonymisation provided that those purposes can be fulfilled in that manner.

5.4 The Company will implement additional safeguards and security measures when Processing Special categories of Personal Data, and will ensure that access to such Data will be limited and restricted only to the Company's authorised HR personnel and, where necessary, employees responsible for the recruitment and management of employees, workers, and consultants and only then when it is necessary to make decisions, which include the consideration of such Data as part of that decision-making process. The types of Special categories of Personal Data Processed by the Company from time to time and the Permitted Purposes and Additional Purposes relied on by the Company for Processing such Data will be set out in any Privacy Notices issued.

6 Consent

6.1 Employment/Workers/officers/consultants.

6.1.1 The Company will only rarely request Consent/Explicit Consent for the Processing of Personal Data/Special categories of Personal Data from its job applicants, employees, workers, officers and consultants. In most cases, Processing will be carried out by the Company relying on one or more other Permitted Purposes or Additional Purposes.

6.1.2 Any historical consent previously embedded in contracts of employment or otherwise which existed prior to the GDPR will no longer be relied on by the Company for the Processing of Personal Data or Special Categories of Personal Data.

6.1.3 Where Consent is requested by the Company of its job applicants, employees, workers, officers or consultants, this will be on an entirely voluntary basis and will not be conditional on that individual's employment, work, consultancy or partnership (as the case may be).

6.1.4 In the event that the Company seeks to request Consent for the purposes of Processing Personal Data/Special categories of Personal Data, the Company will:

6.1.4.1 Ensure that such request is clear and precise and the individual knows clearly what Consent is being sought for;

6.1.4.2 Ensure that the Consent requested is not ambiguous;

6.1.4.3 Ensure that the Consent requires some form of positive action on the part of the individual to signify Consent (the Company will not seek to rely on pre- ticked boxes or silence to signify Consent);

6.1.4.4 Ensure that any Consent request is kept separate from any other terms and conditions of employment/consultancy;

6.1.4.5 Make it clear when requesting Consent that it is voluntary and can be withdrawn at any time and giving details of how to withdraw that Consent;

6.1.4.6 Make it clear what Personal Data/Special categories of Personal Data we will be Processing and for what purpose and for what time frame; and

6.1.4.7 Ensure that any Consent relied on will be regularly reviewed to ensure that it remains relevant and up-to-date.

6.2 Customers, contacts, targets

6.2.1 The Company will Process the Personal Data of customers and business prospects and business targets in accordance with the Company's legitimate interests, and other purposes as set out in any Privacy Notice issued to such customers/business contacts/targets or otherwise as set out in any Privacy Notice appearing on the Company's website. This can include but is not limited to using such Personal Data for marketing purposes and/or keeping you aware of the Company's products and services. In these circumstances, the Company does not require the Consent of existing business clients and business prospects/targets for this purpose.

6.2.2 The Company will, where required, seek the Consent of non-business contacts, consumer targets and other third parties to use their Personal Data for the purpose of marketing the Company's services and business. When such Consent is requested the Company will abide by paragraph 6.1.4

7 Transparency – Privacy Notices

7.1 The Company is required to provide detailed, specific information to Data Subjects when Personal Data is collected about a Data Subject or whenever the reasons for Processing the Personal Data changes. The Company will provide this information to Data Subjects in the form of Privacy Notices. The Privacy Notices will inform the Data Subject of the kind of Personal Data processed by the Company, how such Personal Data is collected and how it will be used, how the Company may process Special categories of Personal Data, the legal basis we will rely on for processing such Personal Data, when we use consent as a basis for processing Personal Data, who we share the Personal Data with, how long we keep it (or the criteria used for determining this) and details of the Data Subject's individual rights under the GDPR.

8 Purpose Limitation

8.1 The Company will not use Personal Data for new, different or incompatible purposes from that disclosed in any Privacy Notice issued to a Data Subject (in accordance with paragraph 7 above).

8.2 In the event that the Company needs to Process Personal Data for new or different purposes from that disclosed, the Company will first issue a revised Privacy Notice to the affected Data Subject explaining the change.

8.3 Employees, workers, officers and consultants who are required to Process Personal Data as part of their duties will report to the Data Manager if they need to Process Personal Data for a different reason to that permitted in the Privacy Notice.

9 Data Minimisation

9.1 The Company will seek to ensure that the Personal Data Processed by the Company is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 Employees, workers, officers and consultants may only Process Personal Data when performing their roles for the Company and the role requires such Processing. Processing of Personal Data is not permitted where such Processing is for any reason unrelated to their duties.

9.3 Employees, workers, officers and consultants must only collect Personal Data that is necessary to fulfil their role for the Company. Excessive and irrelevant Personal Data must not be collected.

9.4 When Personal Data is no longer needed for specified purposes, the Company will delete such Data or anonymise the Data in accordance with the Company's Data retention guidelines and policy. Employees, workers, officers and consultants are expected to follow such retention guidelines and policy.

10 Accuracy

10.1 The Company will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant for the purpose for which we collected it. We will seek to check the accuracy of any Personal Data at the point of collection and at regular intervals thereafter. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10.2 Employees, workers, officers and consultants who are required to Process Personal Data as part of their duties will abide by the principle set out in paragraph 10.1.

11 Storage Limitation

11.1 The Company will seek to ensure that it does not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.2 The Company maintains retention policies and procedures to ensure that Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless the law requires such Data to be kept for a minimum period.

11.3 Employees, workers, officers and consultants are expected to abide by the Company's retention policies and procedures/schedules in respect of the retention of Personal Data.

11.4 The Company will inform Data Subjects of the period for which Data is stored and how that period is determined. This will normally be set out in any Privacy Notice.

12 Security integrity and confidentiality

12.1 The Company has put in place appropriate IT security measures to protect Personal Data that is collected and used by the Company.

12.2 The Company has put in place a variety of security and technical measures to protect the Company's systems and to protect against Data security breaches, including but not limited to: Firewall on all external connections.
Strong passwords (Changed on a regular basis). Regular updating of all computers.
Antivirus software.
Encryption of all devices that leave the premise. Staff training.

12.3 Employees, workers, consultants and officers are responsible for protecting the Personal Data we hold and for ensuring that reasonable and appropriate security measures are used to prevent unlawful or unauthorised Processing of Personal Data or the accidental loss of, or damage to, Personal Data. Particular care must be exercised in protecting Special categories of Personal Data from loss and unauthorised access, use or disclosure.

12.4 Employees, workers, consultants and officers must comply with all applicable aspects of the Company's IT security measures (as referred to in paragraph 12.2 above) and any other policies and procedures communicated from time to time regarding the Processing of Personal Data or IT security. Employees, workers, consultants and officers will comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and other Data Protection Laws and relevant standards to protect Personal Data.

13 IMPORTANT: Reporting a Personal Data Breach

13.1 The Company is required to notify the Information Commissioner of any Personal Data Breach within 72 hours of becoming aware of the Personal Data Breach save where the Personal Data Breach is unlikely to result in the risk to the rights and freedoms of natural persons.

13.2 All employees, workers, officers and consultants are expected to adhere to this paragraph 13. Any breach of this paragraph 13 will be taken seriously and may result in disciplinary action in relation to employees and other action in relation to non-employees. In some instances, serious breaches of this paragraph 13 may be considered to be an act of gross misconduct which could result in the immediate termination of employment, or, as is the case, the immediate termination of any consultancy or engagement.

13.3 If you know or suspect that a Personal Data Breach has occurred you must immediately report this without delay to the Data Manager. To do so, you must either telephone Simon Corbett or email him. The contact details of the Data Manager are: Simon Corbett, Financial Director, email: Simon Corbett, Financial Director whose contact details are: email: simon.corbett@sml-group.co.uk Tel: 0116 4974551 and address: SML Group Ltd, 8 Garden Street, Thurmaston, Leicester, LE4 8DS. When reporting a data breach you must also send a copy to the Company's Managing Director, Thomas Harpin.

13.4 The information you should provide in paragraph 13.3 should where possible include a full description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of individuals concerned and the different types and approximate number of Personal Data concerned. You should also indicate whether you have taken any immediate measures in relation to the Personal Data Breach, and if so, what those measures are.

13.5 You must not report any Personal Data Breach direct to the Information Commissioner (unless involving your own Personal Data), and you must ensure that all reports required under this paragraph 13 are channelled through the Data Manager and other authorised personnel in the first instance who will be responsible for investigating the matter and communicating with the Information Commissioner in this respect.

13.6 You must co-operate in full with any investigation carried out (whether carried out internally or externally and whether by the Company or Information Commissioner) into any Personal Data Breach and must comply promptly with all requests for information from the Company or the Information Commissioner in this respect.

13.7 Unless requested to do so by the Company, you must not attempt to investigate any known or suspected Personal Data Breach yourself. You should notify the Data Manager (and other authorised personnel) immediately in accordance with paragraph 13.3 above and take instruction from the Data Manager and/or others authorised by him/her.

13.8 You must ensure that you preserve all evidence relating to any potential Personal Data Breach. You must not under any circumstances delete any such evidence without being authorised to do so, and in accordance with this policy and the Data Protection Laws.

13.9 You must report all forms of Personal Data Breach to the Data Manager in accordance with this policy whether or not such Personal Data Breaches are of the type that need to be reported to the Information Commissioner. This includes any minor Personal Data Breaches.

13.10 The Company will maintain a record of all Personal Data Breaches, including minor Personal Data Breaches.

13.11 Employees, workers, consultants and officers who are required to process Personal Data will be provided with training from time to time, in accordance with this policy. Such training shall include, but not be limited to how to recognise a Personal Data Breach, steps to take when reporting a Personal Data Breach and how to avoid Personal Data Breaches occurring. If you are unsure about what a Personal Data Breach might be or have any questions regarding Personal Data or how to report a Personal Data Breach you should contact the Data Manager.

14 Transfer limitation

14.1 The GDPR restricts data transfers to countries outside the European Economic Area (EEA). The EEA is made up of all member states of the EU and Norway, Iceland and Liechtenstein.

14.2 In relation to Personal Data, the Company does not transfer any Personal Data outside the EEA and does not authorise any third party to do so.

15 Individual Rights

15.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

15.1.1 Withdraw Consent to Processing at any time (if the Company is using Consent as a legal basis for Processing the Personal Data);

15.1.2 Be informed about the Company's Processing activities. The Company complies with this right by issuing to Data Subject's Privacy Notices from time to time (see paragraph 7 above);

15.1.3 Request access to their Personal Data held by the Company;

15.1.4 Prevent the Company's use of their Personal Data for direct marketing purposes;

15.1.5 Ask the Company to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate Data or to complete incomplete Data;

15.1.6 Restrict Processing in specific circumstances;

15.1.7 Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

15.1.8 Request a copy of any agreement under which Personal Data is transferred outside the EEA;

15.1.9 Object to decisions based solely on Automated Processing, including profiling;

15.1.10 Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

15.1.11 Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

15.1.12 Make a complaint to the Information Commissioner; and

15.1.13 In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

15.2 Any request covered by paragraph 15.1 above should in the first instance be sent to the Data Manager.

16 Accountability

16.1 The Company has implemented appropriate technical and organisational measures in an effective manner, to ensure compliance with the Personal Data protection principles (for principles, see paragraph 4 above).

16.2 The Company, as Data Controller is responsible for, and will be able to demonstrate compliance with the Personal Data protection principles.

17 Record keeping

17.1 The Company will keep records of our processing activities where such processing:

17.1.1 Is likely to result in a risk to the rights and freedoms of Data Subjects;

17.1.2 Is not occasional; or

17.1.3 Includes Special categories of Personal Data or Personal Data relating to criminal convictions and offences.

18 Training

18.1 The Company will ensure that all employees, workers, consultants and officers who are involved in the processing of Personal Data have undergone training to enable them to comply with the Data Protection Laws and this policy.

18.2 Specified Employees, workers, consultants and officers must attend and undergo mandatory training which will be provided by the Company or by authorised trainers on behalf of the Company. Failure to attend such training without reasonable explanation will be considered a disciplinary matter and dealt with in accordance with the Company's Disciplinary Procedure.

19 Automated Processing and Automated Decision-Making

19.1 Automated Decision-Making will not be used by the Company when it has a legal or significant effect on an individual unless:

19.1.1 A Data Subject has provided his or her Explicit Consent;

19.1.2 The Processing is authorised by law; or

19.1.3 The Processing is necessary for the performance of or entering into a contract.

19.2 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects will be informed in any Privacy Notice issued to them.

20 Sharing Personal Data

20.1 Generally, the Company will only share Personal Data with third parties where certain safeguards and contractual arrangements have been put in place.

20.2 The Company will only share Personal Data held by the Company with third party service providers if:

20.2.1 They have a need to know the information for the purposes of providing the contracted services;

20.2.2 Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject;

20.2.3 The third party has agreed to comply with the required data security standards, policies and procedures and out adequate security measures in place;

20.2.4 The transfer complies with any applicable cross border transfer restrictions; and

20.2.5 There is in place a written contract.

21 Changes to this policy

21.1 The Company reserves the right to change this policy at any time without notice.

Date: 01/08/2020

Thomas Harpin
Managing Director