POLICY DOCUMENT

Title:	**Data Protection Policy**
Date:	May 2020
Scope:	All Employees
Statement:	The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The Act and the Directive aim to give individuals rights in connection with the processing of manual and computerised personal data and on the movement of such data. The Company is required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data. This Policy applies to personal data in computerised, manual or any other format, if the data is in a system that allows the information to be readily accessible. The types of personal data that we may process include information about current, past and prospective Employees, client end users, suppliers and other organisations with whom we have dealings. The Company is committed to providing the best possible service to our customers and we will ensure that all personal information is handled fairly and lawfully with due regard to confidentiality and in accordance with the principles of the GDPR.
General Data Protection Regulation (GDPR):	**Justification of Personal Data** We will process personal data in compliance with all six Data Protection Principles. and we will document the additional justification for the processing of sensitive data. **Consent** The data that we collect is subject to active consent by the individual. This consent can be revoked at any time. **Right to be Forgotten** An individual may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies. **Data Audit and Register** Regular data audits to manage and mitigate risks will be included in the Data Register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

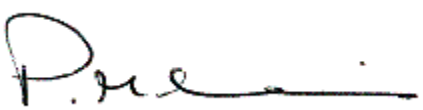
General Data Protection Regulation (GDPR) Continued:	**Reporting Breaches** All employees have an obligation to report actual or potential data protection compliance failures. This allows us to: • Investigate the failure and take remedial steps if necessary. • Maintain a register of compliance failures. **Monitoring** All employees must observe this Policy. The Data Protection Officer has overall responsibility for this Policy. They will monitor it regularly to make sure it is being adhered to.
Data Protection Principles:	Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall 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 are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. e) Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are 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.”

Types of Data:	The GDPR lays down conditions for the processing of any personal data and makes a distinction between personal data and “sensitive” 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. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. Sensitive data is defined as “special categories of personal data”. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual. The Company holds information on: • Employees. • Customers/clients. • Client end users. • Business contacts.
Personal Data Collected and Used:	The Company may collect and use the following types of personal data about you: • Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies. • Your contact details and date of birth. • The contact details for your emergency contacts. • Gender. • Marital status and family details if required for medical insurances purposes. • Information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement. • Bank details and information in relation to your tax status including your national insurance number. • Identification documents including passport and driving licence and information in relation to your immigration status and right to work for us. • Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings). • Information relating to your performance and behaviour at work; • Training records. • Electronic information in relation to your use of IT systems/swipe cards/telephone systems.

'Special Categories of Personal Data':	Special categories of personal data are types of personal data consisting of information as to: • Racial or ethnic origin • Political opinions • Religious beliefs • Trade Union membership • Genetic or Biometric Data • Health • Sexual Orientation • Any Criminal convictions and offenses. The Company may hold and use any of these special categories of your personal data in accordance with the law.
Handling of Personal Sensitive Information:	The Company will, through appropriate management and the use of strict criteria and controls: - • Observe fully the conditions concerning the fair collection and use of personal information. • Specify the purpose for which information is used. • Collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements. • Endeavour always to ensure the quality of information used. • Not keep information for longer than required operationally or legally. • Always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment, protecting personal data held on computers and computer systems by the use of secure passwords which, where possible, are changed periodically and ensuring that individual passwords are not easily compromised). • Ensure that personal information is not transferred abroad without suitable safeguards. • Ensure that the lawful rights of people about whom the information is held can be fully exercised. In addition, the Company will ensure that: • There is someone with specific responsibility for data protection in the organisation (the designated Data Protection Officer). • Reasonable steps are taken to ensure the reliability of Employees having access to personal information. • All Employees managing and handling personal information understand that they are contractually responsible for following good data protection practice. • All Employees managing and handling personal information are appropriately supervised and made aware of their legal responsibilities. • Computer terminals are placed in such a way that screens displaying personal information are not in public view and cannot be seen by passers-by. • That laptops and other portable devices are protected so that information cannot be accessed if they are lost or stolen. • A clear procedure is in place for anyone wanting to make enquiries about handling personal information, whether an Employee or a member of the public and that such enquiries are promptly and courteously dealt with.

Handling of Personal Sensitive Information Continued:	• Methods of handling personal information are regularly assessed and evaluated. By law The Company must provide Employee liability information to any organisation that Employees are transferred to in line with the Transfer of Undertakings Regulations (TUPE).
Sharing Your Personal Data:	We may on occasion share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.
Access to Personal Data:	All individuals with personal data held by the Company are entitled to: • Ask what information we hold about them and why • Ask how to gain access to it. • Be informed how to keep it up to date. • Have inaccurate personal data corrected or removed. • Prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else. • Require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance. • Be informed of what we are doing to comply with our obligations under the GDPR (Regulation (EU) 2016/679). This right is subject to certain exemptions which are set out in the GDPR (Regulation (EU) 2016/679). Any person who wishes to exercise this right should make the request in writing to the Data Protection Officer. We reserve the right to charge the maximum fee payable for each individual access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party. We aim to comply with requests for access to personal information as quickly as possible but will ensure it is provided within 40 days of receipt of a written request. Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any Employee who is in doubt regarding an access request should check with the Director. Information must under no circumstances be sent outside of the UK without the prior permission of the Director.

Employees Responsibilities:	All Employees must ensure that, in carrying out their duties, The Company is able to comply with its obligations under the GDPR. In addition, each employee is responsible for: • Checking that any personal data that s/he provides to us is accurate and up to date. • Informing us of any changes to information previously provided, e.g. change of address. • Checking any information that we may send out from time to time, giving details of information that is being kept and processed. • If, as part of their responsibilities, Employees collect information about other people or about other Employees, they must comply with this Policy. This includes ensuring the information is processed in accordance with the GDPR (Regulation (EU) 2016/679), is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary. • Employees who misuse personal information will be subject to the organisation's disciplinary procedure.
Company Data Protection Officer Responsibilities:	The Company Data Protection Officer is responsible for reviewing this policy and updating the Director on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.
Data Security:	The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All Employees are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.
Publication Of Information:	Information that is already in the public domain is exempt from the GDPR. This would include, for example, information on Employees contained within externally circulated publications such as brochures and other sales and marketing aids. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Director.
Individual's Content:	The need to process data for normal purposes will be communicated to all individuals. Our Contracts of Employment require the consent of Employees to the processing of personal data for the purposes of administering, managing and employing our Employees. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption, etc.) and equal opportunities monitoring. In some cases, if the data is sensitive, for example information on health, race, or gender, express consent to process the data will be obtained. Such processing may be necessary to comply with some of our policies such as Health and Safety and Equal Opportunities. Information about an individual will only be kept for the purposes for which it was originally given.

Data Breaches:	The Company must have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then the Company must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Company must also notify the Information Commissioner's Office within 72 hours. If you are aware of a data breach you must contact Paul Levinson immediately and keep any evidence, you have in relation to the breach.		
Retention and Disposal of Data:	All Employees are responsible for ensuring that information is not kept for longer than necessary. Documents containing any personal information will be disposed of securely.		
Registration:	The Company is registered in the Information Commissioner's public register of Data Controllers. GDPR (Regulation (EU) 2016/679) requires every Data Controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Director is responsible for notifying and updating the Information Commissioner of our processing of personal data.		
Implementation, Monitoring and Review of This Policy:	The Director has overall responsibility for implementing and monitoring this Policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices. Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with the Director who is responsible for ensuring compliance with the GDPR (Regulation (EU) 2016/679) and implementation of this Policy. This Policy is not contractual but indicates how The Company intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action. Any Employee who considers that the Policy has not been followed in respect of personal data about themselves should raise the matter with their Line Manager or the Director.		
Status of Policy:	The Company reserves the right to depart from this Policy where circumstances demand it and to review and vary this Policy from time to time.		
Signed:	 **Paul Levinson** Director	**Dated:**	May 2020