GDPR Policy

Purpose
The aim of this Policy is to lay out clearly how DPS Partnership Ltd controls, holds and processes data in line with the requirements of the **General Data Protection Regulations and the Data Protection Act 2018** (hereafter referred to as GDPR). This is part of our ongoing commitment to be transparent about how we use your data and keep it safe.

DPS Partnership Ltd (hereafter referred to as "The Company") will ensure that it follows the principles contained within the GDPR when dealing with personal and sensitive data:

• Data will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
• Data will be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
• Data held and processed will adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
• Data will be accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
• Data will be 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 and in line with legislative and government recommended requirements for data retention.
• Data will be 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.

Responsibility for Data Privacy
The Company does not require the appointment of a Data Protection Officer for the following reasons:
• The Company is not a "public authority".
• The "core or primary activities" of The company do not require regular and systematic monitoring of data subjects on a large scale.
Responsibility for Data Privacy within the business is held by:
David Kirkup, Director – david@dpsltd.net

David will update the following on a quarterly basis: current policy, the results of internal auditing and implement any changes required.

Data Definitions
Personal Data: This is data that can "identify" a person. Examples include name, photo, email address (personal or business), bank details, medical information etc.
Sensitive Data: This is information relating to medical records, religion, sexual orientation etc. and now also includes genetic and biometric data.

Employee Data
<u>How Employee Data will be used:</u>

As an employer, The Company needs to keep and process information about its employees for normal employment purposes. The information held and processed will be used for management and administrative purposes only and in order to enable The Company to run the business and manage its relationships with its employees effectively, lawfully and appropriately, during the recruitment process, whilst employed, at the time when employment ends and after leaving. This includes using information to enable The Company to comply with its employment contract, to comply with any legal requirements and to pursue its legitimate interests.

It may sometimes be necessary to process employee data to pursue legitimate business interests, for example to prevent fraud, for administrative purposes or in reporting potential crimes. The Company will never process employee data where these interests are overridden by the individuals own interests.

Much of the information we hold will have been provided by employees, but some may come from other internal sources, such as Line Managers, or in some cases, external sources, such as referees.

The type of information held includes (but is not limited to):

• Curriculum Vitae
• References
• Date of Birth
• Passport and Right to Work Information
• Contact and location information (Home address, telephone numbers and email addresses – work and personal).
• Contract of employment and any amendments to it
• Correspondence with or about the employee
• Information needed for payroll, benefits and expenses purposes
• Emergency contact details
• Records of holiday, sickness and other absence
• Records relating to employee career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.
• Computer and Company Mobile Phone use

Employees will, of course, inevitably be referred to in many company documents and records that are produced by the employee and/or and their colleagues in the course of carrying out their duties and the business of the company.

Where necessary, The Company may keep information relating to employees' health, which could include reasons for absence and GP/Occupational Health reports and notes. This information will be used in order to comply with the Company's health and safety and occupational health obligations – to consider how employee health affects their ability to do their job and whether any adjustments to that job might be appropriate. The company also needs this data to administer and manage statutory and company sick pay.

Data Based on Consent

There are two types of employee data that The Company holds and/or processes that will rely on obtaining consent from Employees:

• Employee Photos
• Occupational Health Referrals and GP Medical Report Requests

Where we are processing data based on consent, Employees have the right to withdraw that consent at any time.

Sharing Data with Third Parties

The Company will only disclose information about employees to third parties if legally obliged to do so or if it needs to comply with its contractual duties to its employees, for instance, if it is required to pass on certain information to an external payroll provider, pension provider or health insurance schemes.

Employee personal data will be stored for a period of 6 years following employment end, after which it will be securely shredded.

If The Company intends to process employee personal or sensitive data for a purpose other than that which it was collected the employee will be provided with information on that purpose and any other relevant information.

Customer Data

How Customer Data will be used:

The Company needs to keep and process information about its customers for ongoing business and contact purposes. The information held and processed will be used for service provision and administrative purposes only and in order to enable The Company to run the business and manage its relationships with its customers effectively, lawfully and appropriately.

The type of information held includes (but is not limited to):

• Customer Name and Company Name
• Contact details (telephone numbers, address and email addresses).
• Records and notes of customer meetings/discussions held.

Sharing Data with Third Parties

The Company may be required to share customer data (limited to contact and location details) with third party processors (such as courier companies).

The Company will not share customer data with any third-party processor for any purpose other than for legitimate business interests and provided these are not overridden by the interests of the Customer.

The Rights of the Individual

Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) all individuals have a number of rights with regard to their personal data. All individuals have the right to request from the Company access to and rectification or erasure of personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

Data Subject Access Requests (DSAR)

Individuals are allowed access to their personal data. The Company will provide a copy of this information free of charge, however, if requests are considered to be manifestly unfounded, excessive or repetitive; the Company will consider charging the individual a reasonable fee.

Any Data Subject Access Requests must be made in writing to The Company. The Company will respond within one month of receiving this DSAR. However, should such a request be complex or numerous, The Company will reserve the right to extend this period to a further two months.

Individuals have the right to lodge a complaint to the Information Commissioners' Office if they believe that that The Company has not complied with the requirements of the GDPR or the Data Protection Act 2018 with regard to their data.

The Right of Erasure

The right of erasure does not mean provide the individual with a "right to be forgotten". Individuals can request for personal data to be erased or to prevent processing in the following circumstances:

• Where data is no longer necessary in relation to the purpose for which it was originally collected/processed.
• When the individual withdraws consent (applies only to data where consent is required for processing).
• Where there is no legitimate interest for continuing the processing.
• If the data was unlawfully processed.
• To comply with a legal obligation.

There are some circumstances where The Company can refuse to comply with a request for erasure; this will be dependent on the type of data and the processing need.

Data Security

The Company takes the security of its data seriously. All processing and storage of data is subject to suitable security precautions relevant to the type and use of that data.

We protect the privacy of your information using highly secure, password-protected servers. The online and offline security measures we adopt protect information we have against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of or damage to personal data.

Any credit card or personally identifying information divulged to The Company via our website will be stored on secure servers and not released to any other party without your explicit written authorisation.

Pages on our website that request payment information are protected using SSL (Secure Socket Layer) security, which encrypts any data transmitted. Once you enter a credit/charge card number, we will never display the entire card number if the page is recalled after you have submitted it. This also covers the use of the "Back" button on your browser. The inner digits will always be displayed as asterisks, protecting your card number from other users of your computer or anyone who happens to see the screen.

Data Breaches

The investigation and reporting of Data Breaches are the responsibility of the Data Privacy Committee and will be reported to the Information Commissioners Office in accordance with the reporting requirements of GDPR and the Data Protection Act 2018.