Data Protection Privacy Notice (Engagement)

This notice explains what personal data (information) we hold about you, how we collect it, how we use and how we may share information about you during your assignment (or employment) and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Who collects the information

The recruitment businesses operating under 'Rocket Staffing Group' are 'data controllers' and we gather and use certain information about you. This information is also used by our affiliated entities and group companies, further information can be obtained via our website www.rocketstaffing.co.uk and so, in this notice, references to 'we' or 'us' mean the Company and our group companies.

Data protection principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

About the information we collect and hold

We may collect the following information during your work with us:

- Your name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e. name, relationship and home and mobile phone numbers);
- Information collected during the recruitment process that we retain during your employment;
- Assignment contract information;
- Details of pay and benefits, bank/building society, National Insurance and tax information, your age;
- Details of your spouse/partner and any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- A copy of your driving licence;
- Details of any incentive arrangements, and all information included in these and necessary to implement and administer them;
- Details of your pension arrangements, and all information included in these and necessary to implement and administer them;
- Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health);
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
- Criminal records information, including the results of Disclosure and Barring Service (DBS) checks or Disclosure Scotland;
- Any trade union membership;
- Information on grievances or complaints raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals and performance reviews;
- Details of your performance management/improvement plans (if any);
- Details of your time and attendance records;

- Information regarding your work output;
- Photos or videos of you that we may use and share with clients, internally or for social media;
- Information in applications you make for other positions with any other of our clients or internally;
- Information about your use of our IT, communication and other systems, and other monitoring information;
- Details of your use of business-related social media, such as LinkedIn;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur); and
- Details in references about you that we give to others.

Some of the categories above may not apply to you. The data that we collect and retain varies depending on the role you are performing and the sector that you operate in.

How we collect the information

We may collect this information from you, your personnel records, our clients where you are assigned, the Home Office, scheme administrators, pension administrators, your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators, the DBS, your trade union, other employees, consultants and other professionals we may engage, e.g. to advise us generally and/or in relation to any grievance, complaint, conduct appraisal or performance review procedure, our or our clients (the following) payroll system, our CRM system, payroll partners including external umbrellas, HR system, activity monitoring software, automated monitoring websites and other technical systems, such as computer networks and connections, CCTV and access control systems, communications systems, remote access systems, trading platforms, email and instant messaging systems, intranet and Internet facilities, telephones, voicemail, mobile phone records.

Why we collect the information and how we use it

We will typically collect and use this information for the following purposes (other purposes that may also apply are explained in our data protection policy):

- for the performance of a contract with you, or to take steps to enter into a contract;
- for compliance with a legal obligation (e.g. our obligations to you as your employer under employment protection and health safety legislation, and under statutory codes of practice, such as those issued by Acas); and
- for the purposes of our legitimate interests or those of a third party (such as a benefits provider), but only if these are not overridden by your interests, rights or freedoms.

Further information on the monitoring we undertake in the workplace and how we do this is available in from our HR Department.
We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

How we may share the information

As part of a Group of recruitment agencies we may share your data with other internal Group Companies depending upon the job role you are applied for or are engaged in.

We may need to share some of the above categories of personal information with other parties, such as clients & companies who have job roles that you are interested in or wish to apply to work for, trade associations such as the REC, external payroll

bureaus (but only as relevant and applicable to the role applied for), HR consultants, third party auditors and professional advisers. Depending upon the purpose and recipient of the information it may be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

Where information may be held

Information may be held at our offices and those of our group companies, our clients, third party agencies, service providers, representatives and agents as described above. We have security measures in place to seek to ensure that there is appropriate security for information we hold**.**

How long we keep your information

We keep your information during and after your assignment (or employment) for no longer than is necessary for the purposes for which the personal information is processed unless otherwise agreed with you. Note that as we also offer work finding services your information may be retained for a period for up to two years with a view to securing you further assignments which we may contact you about.

Your rights to correct and access your information and to ask for it to be erased

Please contact our HR Department on hr@jarell.co.uk if you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask our Data Protection Officer for some but not all of the information we hold and process to be erased (the 'right to be forgotten') in certain circumstances. Our Data Protection Officer will provide you with further information about the right to be forgotten, if you ask for it.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.