14 Data Protection

1. Overview

1.1. During the course of its business activities the Company and its Employees are involved in collecting and storing personal information about our staff and other individuals (or 'Data Subjects').

1.2. It is important that the Company (as the 'Data Controller') treats this information in an appropriate and lawful manner and that employees who have responsibility for the storing and processing of personal information understand and comply with relevant legal obligations.

2. Accountability

2.1. The Data Protection Compliance Officer (DPCO) has ultimate responsible for ensuring compliance with the Data Protection Act and any successor legislation and this Policy. The DPCO is Tracey Jones.

2.2. Any questions or concerns about data retention or processing should be referred to the DPCO.

2.3. The DPCO will ensure that the Company's employees are aware of their obligations and appropriately trained.

2.4. The DPCO will review the following areas on a regular basis:

- The kinds of personal information retained and any changes to this
- The location and method of storing this data
- Details of the security measures (e.g. password protection, encryption, etc) used to safeguard this data and any changes to this
- Where the data originated (e.g. the data subject or a third party)
- What the basis for retaining or processing the data is (i.e. data subject consent or some other legal basis)
- How and why this data is processed
- Who has access to this data and why they are permitted access
- Where applicable, the adequacy of contracts with suppliers to ensure that they comply with data protection laws
- Measures taken to minimise the data items that are retained and processed
- Measures taken to ensure the accuracy of data
- Measures taken to delete data in relation to which consent and / or lawful reasons for retention no longer apply
- Steps taken to ensure that those who report to them are adequately trained in relation to data protection and reminded of their obligations from time to time

3. Personal Information

3.1. Personal Information is information which:

- Is about a Data Subject and affects that person's privacy (whether personal or professional) in that the information has the personal as its focus or is otherwise biographical in nature, and
- Identifies the Data Subject (either by direct reference or is capable or identifying them together with other information).

4. Data Processing

4.1. Personal information may only be processed fairly, lawfully.

4.2. In additional to fairness and lawfulness one or more of the following must also apply:

- The data subject has consented
- The Company needs to process the data because of a legitimate interest of the Company or a third party to whom it is disclosed, and that this interest is warranted when the rights and interests of the data subject are considered
- The processing is necessary in relation to a contract that the data subject has entered into, or because they have asked the Company to do something so they can enter into a contract (e.g. completed an application form)
- The processing is necessary because of a legal obligation placed on the Company (e.g. in relation to the right to work in the UK, deduct PAYE and NICs, etc)
- The processing is necessary to protect the data subject's vital interests (i.e. the need to disclosure medical details in a case of life or death)

4.3. Sensitive Personal Data relates to a data subject's racial origins, political opinions, religious beliefs, trade union membership, health, sex life and convictions.

4.4. Sensitive Personal Data may only be processed if one or more of the following conditions is met in addition to those set out above:

- The data subject has given explicit consent to the processing
- The processing is necessary to comply with employment law
- The processing is necessary to protect the vital interests of the data subject or another
- The processing is carried out by a not-for-profit organisation and does not involve disclosing data to a third party
- The data subject has deliberately made the information contained within the data public
- The processing is necessary in relation to legal proceedings or taking legal advice
- The processing is necessary for medical purposes
- The processing is necessary for equal opportunities monitoring
- The processing is specifically authorised by law (e.g. for preventing or detecting crime)

5. The Data Protection Principles

5.1. The Company must ensure that information it holds concerning individuals is processed according to the Data Protection Principles, which are as follows.

5.2. Data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to countries without adequate protection

5.3. Data Subjects should know that the Company holds their information and the reasons why it is being held.

5.4. You may be involved in processing personal information as part of your job.

5.5. At all times you must keep all personal information confidential and secure, and take particular care not to disclose it to any other person (whether inside or outside the Company) unless authorised to do so.

5.6. You should take particular care not to disclose personal information held by the Company over the telephone or otherwise orally unless you are totally confident of the other person's identity and that they are entitled to receive the information. If you are in any doubt you should seek assistance from the DCPO.

5.7. You are required to assist the Company in ensuring that data is used in accordance with the Data Protection Principles.

5.8. Do not use any personal data except as authorised by the Company for the purposes of undertaking the duties and responsibilities of your job role.

5.9. If you identify that the Company maintains unnecessary or inaccurate personal information the DPCO should be informed of this. This includes notifying us if data held by us that relates to you changes (e.g. your address or personal mobile phone number).

6. Data Breaches and Safeguards

6.1. If you consider that this Policy has not been followed (either by yourself or anyone else) you should bring this to the attention of your Line Manager or the DCPO without delay.

6.2. Any Employee who identifies inappropriate use or disclosure of any Sensitive Personal Data should inform the DPCO immediately and pass responsibility for the same to that person.

6.3. The Company / DCPO will reach quickly to any data breach and take the following actions:

- Establish what data is involved in the breach
- Take such steps as are necessary to secure the data in question
- Act to prevent any further or repeat of the data breach
- Report the fact of the data breach to the ICO where this is required and within the prescribed time limit
- Report the fact of the data breach to any affected data subject without undue delay

6.4. The DPCO will review the Company's practices, policies and procedures regularly to ensure they are fit for purpose and fully compliant.

6.5. As part of this review the DCPO will:

- review the areas in paragraph 2.4 above and summarise them in a single report, and

- undertake a privacy impact assessment to review any processing activities that present a serious risk of breach and take steps to address any specific concerns.

6.6. Compliance with data protection laws is of fundamental importance to the Company, however, it is acknowledged that mistakes are made innocently and it is of equal importance that a culture of transparency and honesty prevails so that errors are recognised, rectified and avoided in the future. Accordingly, no employee will face detrimental treatment or disciplinary action for a breach of this policy that is unintentional and disclosed to their manager and / or the DCPO without delay.

7. Privacy Notice

7.1. We process the following kinds of information in relation to Employees and Workers:

- Date of birth
- Gender
- Nationality
- Signature
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date
- Location of employment or workplace
- Copies of driving licence and/or passport
- Qualification certificates
- Reference details and their opinions about your performance in former roles
- Recruitment information (including copies of right to work documentation, and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Pay history
- Performance information including probation forms, appraisals and promotions
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipecard records
- Information about your use of our information and communications systems
- Photographs
- P45 documents
- Signed terms of employment or engagement
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences

8. Why do we process this information?

We will use the types of personal information specified above in the following circumstances:

8.1. Where we need to perform the contract we have entered into with you.

8.2. Where we need to comply with our legal obligations.

8.3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

9. Situations in which we will use your personal information

9.1. We need the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

9.2. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee, deducting tax and National Insurance contributions
- Providing benefits to you
- Liaising with your pension provider
- Administering the contract we have entered into with you
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- Equal opportunities monitoring

- Statutory Sick Pay / Sick Pay
- Maternity Rights
- To assess your capacity on health grounds subject to appropriate confidentiality safeguards
- To comply with our duty of care and to consider work related adjustments where required under the Equality Act 2010

9.3. Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

9.4. We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

10. Where did we collect this data from?

10.1. We usually only collect information for Data Subjects directly. But in the context of employment, we may also have obtained your data from one of the sources below.

- Employment agencies or businesses
- The Disclosure and Barring Service (DBS)
- Former employees or workers who may have recommended you

10.2. We will also collect information in the categories above in the course of your employment throughout the period you work for us.

11. Are you under any obligation to provide the Personal Data?

11.1. Where we process Personal Data to comply with our legal obligations Data Subjects must provide this information.

11.2. If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our employees /workers), or we may be prevented from achieving our legitimate interests as your employer.

12. Who do we share this information with?

12.1. We use some third-party service providers who process data for us under strict instructions and under a binding contract ("Processors"). Our Processors provide the following services:

- Payroll
- Pension administration
- IT services
- Cloud-based storage
- Outsourced HR

- Data Protection Consultancy
- Legal advisors
- Accountancy services

12.2. All our Processors are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

12.3. We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

12.4. You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

13. How long do we keep this information?

13.1. We retain Personal Data in compliance with our Retention Policy and Schedule for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

14. How do we keep this information secure?

14.1. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

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

15. What rights do you have?

15.1. Data Subjects are entitled to request that we erase, restrict, rectify or provide you with a copy of the data we hold, and may object to processing activities.

15.2. If we process Personal Data on the basis of Consent, the Data Subject may withdraw their Consent in respect of the particular processing activity.

15.3. It is our policy to fulfil any such request within the statutory period of one month unless there is a compelling legal or contractual obligation which prevents us from doing so.

15.4. To make any such request please contact our DPCO Tracey Jones.

15.5. You also have the right to lodge a complaint with the UK's data regulator, the Information Commissioner's Office. Visit www.ico.org for more information.

15.6. Our contact information

Simon Jones Superfreight Ltd

170 Rowan Road, London, SW16 5BN

0207 924 3933

Policy Adopted Date:	01/09/18
Due for Review Date:	01/09/20