Data Protection Policy

1. Introduction

1.1. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. This policy sets out the things we must tell you about data protection including the types of information we collect about you and how we use it.

1.2. We take the security and privacy of your data seriously and intend to comply with our legal obligations under the *Data Protection Act 2018* (2018 Act) and the *EU General Data Protection Regulation* (GDPR) in respect of data privacy and security.

1.3. This policy applies to current and former employees, workers, and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract and any other notice we issue to you from time to time in relation to your data.

1.4. The Company is a 'data controller' for the purposes of your personal data. This means that we decide how and why we process your personal data.

1.5. This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

1.6. This policy does not form part of your contract and we reserve the right to amend this policy at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR.

2. Data protection principles

2.1. Personal data must be processed in accordance with the following 'data protection principles:

a Be processed fairly, lawfully and transparently

b Be collected and processed only for specified, explicit and legitimate purposes

c Be adequate, relevant and limited to what is necessary for the purposes for which it is processed

d Be accurate and kept up to date. Any inaccurate data must be deleted or rectified

e Not be kept for longer than is necessary for the purposes for which it is processed

f Be processed securely

2.2. We are responsible for ensuring and demonstrating compliance with these principles.

3. How we define personal data

3.1. 'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person. It does not include anonymised data.

3.2. This policy applies to all personal data, whether it is stored electronically, on paper or in/on other materials.

3.3. This personal data might be provided to us by you or by someone else (such as a former employer, a medical practitioner or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of your contract, or after it has ended. It could be created by your line manager or other colleagues.

3.4. We will collect and use the following types of personal data about you:

a Recruitment information, such as your application form, CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.

b Your contact details and date of birth.

c The contact details for your emergency contacts.

d Your gender.

e Your marital status and family details.

f Information about your contract, including start and end dates, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement.

g Your bank details and information in relation to your tax status, including your National Insurance number.

h Your identification documents, including your passport and driving licence and information in relation to your immigration status and right to work for us.

i Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings).

j Information relating to your performance and behaviour at work.

k Training records.

l Electronic information in relation to your use of IT systems/on board computers/swipe cards/telephone systems.

m Your images (whether captured on CCTV, in-vehicle camera, video or by photograph).

n Any other category of personal data for which we have a lawful basis for processing.

4. How we define special categories of personal data

4.1. GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection. 'Special categories of personal data' are types of personal data consisting of information about:

a Your racial or ethnic origin

b Your political opinions

c Your religious or philosophical beliefs

d Your trade union membership

e Your genetic or biometric data

f Your health

g Your sex life and sexual orientation

4.2. We may hold and use any of these special categories of your personal data in accordance with the law.

4.3. We may hold and use personal data relating to criminal allegations, offences, proceedings and convictions.

5. How we define processing

5.1. 'Processing' means any operation which is performed on personal data, such as:

a Collection, recording, organisation, structuring or storing

b Adaption or alteration

c Retrieval, consultation or use

d Disclosure by transmission, dissemination or otherwise making available

e Alignment or combination

f Restriction, destruction or erasure

5.2. 'Processing' includes processing personal data which forms part of a filing system and any automated processing.

6. How will we process your personal data?

6.1. We will process your personal data (including special categories of personal data) in line with our obligations under the 2018 Act.

6.2. We will use your personal data:

a To perform the contract between us

b To comply with any legal obligation

c If it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop using your personal data. See details of this in section 12.

6.3. We can process your personal data for the purposes listed directly above without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

6.4. We may use you data for any other purpose in circumstances where you have given your consent.

6.5. If you choose not to give us certain personal data, we may not be able to carry out some parts of the contract between us. For example, if we do not have your bank account details, we will not be able to pay you. It might also prevent us from complying with certain legal obligations and duties, such as paying the right amount of tax to HMRC or making reasonable adjustments in relation to any disability you may have.

7. Examples of when we might process your personal data

7.1. We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.2. For example:

a To decide whether to employ (or engage) you

b To decide how much to pay you and the other terms of your contract with us

c To check you have the legal right to work for us

d To carry out the contract between us, including, where relevant, its termination

e To train you and review your performance

f To decide whether to promote you

g To decide whether and how to manage your performance, absence or conduct

h To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else

i To determine whether we need to make reasonable adjustments to your workplace or role because of your disability

j To monitor diversity and equal opportunities

k To monitor and protect the security (including network security) of the Company, you, other colleagues, our customers and others

l To monitor and protect your health and safety and that of our other colleagues, our customers and third parties

m To pay you and provide pension and other benefits in accordance with the contract between us

n To pay tax and National Insurance

o To provide a reference upon request from another employer

p To pay trade union subscriptions

q To monitor compliance by you, us and others with our policies and our contractual obligations

r To comply with employment law, immigration law, health and safety law, tax law and other laws which affect us

s To answer questions from insurers in respect of any insurance policies which relate to you

t To run our business and plan for the future

u For the prevention and detection of fraud or other criminal offences

v To defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure

w For any other reason where we have a lawful basis.

7.3. We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we ask for your consent to process a special category of personal data, then we will explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose to by contacting our Data Protection Officer; Mike Linney.

7.4. We do not need your consent to process special categories of your personal data when we process it for the following purposes:

a Where it is necessary for carrying out rights and obligations under employment law.

b Where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent.

c Where you have made the data public.

d Where processing is necessary for the establishment, exercise or defence of legal claims.

e Where processing is necessary for the purposes of occupational health or for the assessment of your working capacity.

7.5. We might process special categories of your personal data for the purposes in paragraph 7.2 in relation to:

a Your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities.

b Your sickness absence, health and medical conditions to monitor your absence; assess your fitness for work; pay you benefits; comply with our legal obligations under employment law, including making reasonable adjustments; and look after your health and safety.

c Your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

8. Sharing your personal data

8.1. Sometimes, we might share your personal data with customers, suppliers or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

8.2. We require those people and 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.

9. How should you process personal data for the Company?

9.1. Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this and other relevant policies.

9.2. The Company's Data Protection Officer is responsible for reviewing this policy and updating the board of directors 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 the DPO.

9.3. You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

9.4. You should not share personal data informally.

9.5. You should keep personal data secure and not share it with unauthorised people.

9.6. You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own details change.

9.7. You should not make unnecessary copies of personal data, and you should keep and dispose of any copies securely.

9.8. You should use strong passwords.

9.9. You should lock your computer screens when not at your desk.

9.10. Personal data should be encrypted before being transferred electronically to authorised external contacts.

9.11. Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

9.12. Do not save personal data to your own personal computers or other devices.

9.13. Personal data should never be transferred outside the European Economic Area except in compliance with the law and with the authorisation of the DPO.

9.14. You should lock drawers and filing cabinets. Do not leave documents that contain personal data on your desk or anywhere else that can be accessed by unauthorised people.

9.15. You should not take personal data away from Company's premises without authorisation from your line manager or the DPO.

9.16. Personal data should be shredded and disposed of securely when you have finished with it.

9.17. You should seek support from the DPO if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

9.18. Any deliberate or negligent breach of this Policy by you may result in disciplinary action being taken against you.

9.19. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our Disciplinary Policy, and you could be dismissed.

10. How to deal with data breaches

10.1. If this policy is followed, we should not have any data breaches. But if a breach of personal data occurs (whether in respect of you or someone else), then we must take notes and keep evidence of that breach. If the breach is likely to pose a risk to the rights and freedoms of individuals, then we must notify the Information Commissioner's Office within 72 hours, where feasible. If the breach is likely to result in a high risk to your rights and freedoms, then we will let you know about it.

10.2. If you are aware of a data breach, then you must contact the DPO immediately and keep any evidence you have in relation to the breach.

11. Subject access requests

11.1. Data subjects can make a 'subject access request' (**SAR**) to find out what information we hold about them. This request must be made in writing. If you receive a SAR, you should forward it immediately to the DPO and HR who will coordinate a response.

11.2. To make a SAR in relation to your own personal data, you should write to the DPO. We must respond within one month unless the request is complex or numerous, in which case the period in which we must respond can be extended by up to two months.

11.3. There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request. We normally work on the basis that any request which will take more than a day to deal with is likely to be manifestly excessive, and in those circumstances, will be discussed with you.

12. Your data subject rights

12.1. You have the right to information about what personal data we process, how we process it and on what basis, as set out in this Policy.

12.2. You have the right to access your own personal data by way of a SAR.

12.3. You can correct any inaccuracies in your personal data by contacting the DPO.

12.4. You have the right to request that we erase your personal data where we were not entitled under law to process it or where it is no longer necessary to process the data for the purpose for which it was collected. You can request erasure by contacting the DPO.

12.5. During the process of requesting that your personal data be corrected or erased, or while you are contesting the lawfulness of our processing, you can ask for the data to be used in a restricted way only. To do this, contact the DPO.

12.6. You have the right to object to data processing where we rely on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

12.7. You have the right to object if we process your personal data for the purposes of direct marketing.

12.8. You have the right to receive a copy of your personal data and, with some exceptions, to transfer your personal data to another data controller.

12.9. You have the right to be notified of a data security breach concerning your personal data where that breach is likely to result in a high risk of adversely affecting your rights and freedoms.

12.10. In most situations, we will not rely on your consent as a lawful ground to process your data. If we do request your consent to process your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the DPO.

12.11. You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details, including a helpline number, can be found on the Information Commissioner's Office website (www.ico.org.uk). The Information Commissioner's Office website has more information on your rights and our obligations.

13. Data retention

13.1. We will only retain personal data and sensitive data for as long as necessary for the purposes for which we collected it. After this time, it will be deleted or archived.

14. Useful links and contacts

14.1. Our DPO at the time of publication of this Policy is Mike Linney. Our DPO can be contacted via data.protection@oxalis-logistics.com

14.2. Useful information and guidance about the matters covered in this policy can be found on www.ico.org.uk.