CARLTON

PRIVACY POLICY FOR EMPLOYEES, WORKERS AND CONSULTANTS

This policy applies to all staff of Carlton Limited and its subsidiaries (the "Carlton" Group of Companies).

1 Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, workers, volunteers, interns 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 of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.3 The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.4 This policy explains how the Company 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.

1.5 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 The Company will comply with the data protection regulations which provides that personal data must be:

- processed fairly, lawfully and transparently;
- collected and processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;

- accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed securely.

3 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 and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 We will collect, store and use the following types of personal data about you:

- recruitment information such as your CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- 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;
- your bank details and information in relation to your tax status including your national insurance number;
- your 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;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which we may notify you of from time to time.

3.3 We may also collect, store and use '**special categories of personal data**' consisting of information as to:

- your racial or ethnic origin;

- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

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

4 Collecting personal data

4.1 We collect personal data from you or from third parties (such as a former employer, an employment agency, your doctor, or a credit reference agency), or it could be created by the Company. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

4.2 If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

5 Processing personal data

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

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

5.2 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

5.3 Most commonly, the Company will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else) and your interests and fundamental rights do not override those.

5.4 The Company may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests); or
- Where it is needed in the public interest.

5.5 Please note that we may process your personal data for the purposes set out at paragraphs 5.3 and 5.4 above without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

6 Examples of when we might process your personal data

6.1 We need all the categories of personal data listed at paragraph 3.2 above for various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement), but primarily to allow us to perform our contract with you and to enable us to comply with our legal obligations. In some cases we may use your personal data to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

6.2 The situations in which we will process your personal data are listed below:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability;
- to monitor diversity and equal opportunities;

- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties;
- to pay you and provide pension and other benefits in accordance with the contract between us;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us;
- to answer questions from insurers in respect of any insurance policies which relate to you;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure;
- to provide information within any tender or bid process as required; and
- for any other reason which we may notify you of from time to time.

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

6.4 We will only use your personal data for the purposes for which we collected it. If we need to use your personal data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so. 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.

7 Examples of when we might process special categories of personal data

7.1 Special categories of personal data (see paragraph 3.3 above) require higher levels of protection.

7.2 We may process special categories of personal data in the following circumstances:

- in limited circumstances, with your explicit written consent;
- where we need to carry out our legal obligations or exercise rights in connection with employment; or
- where it is needed in the public interest.

7.3 Less commonly, we may process special categories of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

7.4 A non-exhaustive list of situations in which we will process special categories of personal data are listed below:

- your race, national or ethnic origin, religion, philosophical or moral beliefs, sexual orientation or gender may be processed to ensure meaningful equal opportunities monitoring and reporting;
- information relating to leaves of absence, which may include sickness absence or family related leaves may be processed to comply with our legal obligations under employment law;
- information about your physical or mental health, disability status and/or and medical conditions may be processed to monitor and manage sickness absence, to assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

7.5 We do not need your consent if we use special categories of your personal data in accordance with this policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

8 Automated decision-making

8.1 We do not envisage that you will 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.

9 Sharing your personal data

9.1 Sometimes we may have to share your personal data with clients or our contractors and agents, including third-party service providers to carry out our obligations under our contract with you or for our legitimate interests.

9.2 We require those companies to take appropriate security measures 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.

9.3 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

10 Data security

10.1 We have robust measures in place (as set out in this policy) to minimise and prevent data breaches from taking place.

10.2 Should a breach or suspected breach of personal data occur (whether in respect of you or someone else) then will notify you and any applicable regulator where we are legally required to do so.

10.3 If you are aware of (or suspect) a data breach you must contact the Data Protection Manager immediately and keep any evidence you have in relation to the breach.

11 Data retention

11.1 We will only retain your personal data 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. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk or harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

11.2 In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal data in accordance with applicable laws and regulations.

12 Your obligations as an employee, contractor or worker

12.1 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 policy.

12.2 The Company's Data Protection Manager is responsible for reviewing this policy and updating the Company in relation to its 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 Data Protection Manager.

12.3 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.

12.4 You should not share personal data informally.

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

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

12.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

12.8 You should use strong passwords.

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

12.10 You should consider encrypting personal data before transferring it electronically to authorised external contacts.

12.11 You should consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

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

12.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Manager.

12.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

12.15 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Manager.

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

12.17 You should ask for help from our Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

12.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

12.19 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 procedure, which could result in your dismissal.

13 Subject access requests

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

13.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Protection Manager. We will endeavour to respond within one month unless the request is complex or numerous in which case we may need this period to be extended by a further two months.

13.3 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.

14 Your data subject rights

14.1 In certain circumstances, by law you have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).

- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

- Object to processing of your personal data for direct marketing purposes.

- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.

- Request the transfer of your personal data to another data processor.

14.2 If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another data processor, please contact the Data Protection Manager in writing.

14.3 You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

14.4 You have the right to complain to the Information Commissioner. You can do this be 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). This website has further information on your rights and our obligations.

14.5 Where you have provided your consent to the collection, processing and transfer of your personal data, you have the right to withdraw your consent for specific processing at any time. To withdraw your consent, please contact the Data Protection Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

15 Data Protection Manager

15.1 If you have any questions about this privacy notice or how we handle your personal data, please contact the Data Protection Manager, Nicolas Ollivant.

Version Control and Summary of Changes

Version Number	Date	Comments (description change and amendments)
1	29.05.18	New policy – Board approved