DATA PROTECTION POLICY

1. Policy Statement

Every day our business will receive, use and store personal information about our clients, suppliers and colleagues. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection legislation.

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. About This Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data we collect or process.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Iain McBride, Director is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to them in the first instance or reported in line with the organisation's Whistleblowing Policy or Grievance Policy.

3. What is Personal Data?

Personal data means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. Data Protection Principles

Anyone processing personal data, must ensure that data is:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and any further processing is completed for a compatible purpose.
c. Adequate, relevant and limited to what is necessary for the intended purposes.
d. Accurate, and where necessary, kept up to date.
e. Kept in a form which permits identification for no longer than necessary for the intended purposes.
f. Processed in line with the individual's rights and 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.
g. Not transferred to people or organisations situated in countries without adequate protection and without firstly having advised the individual.

5. Fair and Lawful Processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest

of the business.

6. Processing for Limited Purposes

In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Notifying Individuals

If we collect personal data directly from an individual, we will inform them about:

a. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
b. Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
c. The types of third parties, if any, with which we will share or disclose that personal data.
d. The fact that the business intends to transfer personal data to a non-EEA country or international organisation and the appropriate and suitable safeguards in place.
e. Information about the period that their information will be stored.
f. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
g. Their right to object to processing and their right to data portability.
h. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
i. The right to lodge a complaint with the Information Commissioners Office.
j. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
k. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, or for our legitimate interests as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.

We will inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. Adequate, Relevant and Non-excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

11. Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

a. Confirmation as to whether or not personal data concerning the individual is being processed.
b. Request access to any data held about them by a data controller (see also *Clause 14 Subject Access Requests*).
c. Request rectification, erasure or restriction on processing of their personal data.
d. Lodge a complaint with a supervisory authority.
e. Data portability.
f. Object to processing including for direct marketing.
g. Not be subject to automated decision making including profiling in certain circumstances.

12. Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a. **Confidentiality** means that only people who are authorised to use the data can access it.
b. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
c. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Company's central computer system instead of individual PCs.

Security procedures include:

a. **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
b. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
c. **Data minimisation.**
d. **Pseudonymisation and encryption of data.**
e. **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
f. **Equipment.** Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. Disclosure and Sharing of Personal Data

We may share personal data for our legitimate interests with the following:

a. External Advisors
b. Government departments and financial institutions
c. Other companies within our Group (if applicable)
d. ANY OTHER EXAMPLES THAT YOU CAN ADVISE ON

14. Subject Access Requests

Individuals must make a formal request for information we hold about them to:

Iain McBride, Director
iain@macrecruit.co.uk

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
b. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

Where a request is made electronically, data will be provided electronically where possible.

15. Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

PRIVACY NOTICE – EMPLOYEE DATA

How your information will be used

1. As your employer, the Company needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

2. As a company pursuing recruitment and head hunting activities, we may sometimes need to process your data to fulfil our legal obligations or pursue our legitimate business interests, for example for administrative purposes. We will never process your data where these interests are overridden by your own interests.

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

4. The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits and expenses purposes; contact and emergency contact details; records of holiday, sickness and other absence; information needed for equal opportunities monitoring; and records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records. Closed circuit television (CCTV) images are retained for 90 days in line with insurance requirements after which, unless required for a legitimate reason, they will be destroyed.

5. Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay.

6. We only process special categories of information relating to your religious and philosophical beliefs as required by law.

7. In addition, we monitor computer and telephone/mobile telephone use, as detailed in our Employee Handbook.

8. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you or to allow us to pursue our legitimate business interests, for instance we may need to pass on certain information to HMRC, our external company accountant or legal / HR advisors or pension schemes.

9. In limited and necessary circumstances, your information may be transferred outside of the EEA or to an international organisation to comply with our legal or contractual requirements. We have in place the following safeguards to ensure the security of your data:

    a. Adequacy Decisions: The European Commission can determine that a non-EEA country offers an adequate level of data protection. If a country has received an adequacy decision, personal data can be transferred from the EEA to that country without any further safeguard.
    b. International Data Transfer Agreements: These are agreements between the data exporter and data importer that include provisions to ensure the protection of personal data.
    c. Transfer Risk Assessment: This assessment will help identify and mitigate potential risks.

10. The personal data we hold on our employees falls into a variety of categories for example payroll records, health and safety records and employment records. Some of these we need to retain for a statutory period and others we retain for set periods for legitimate reasons. Details of our retention periods are contained at the end of this document.

11. If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.

Your rights

12. Under the Data Protection legislation you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

13. If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

14. You have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the Data Protection legislation with regard to your personal data.

Identity and contact details of data controller

15. Iain McBride is the controller of data.

16. If you have any concerns as to how your data is processed you can contact:

Iain McBride, Director
iain@macrecruit.co.uk

HR RECORDS – RETENTION PERIODS

Payroll related records

- **Accident Books / Accident Records/Reports** – 3 years from the date of the last entry
- **Accounting Records** – 3 years for private companies / 6 years for public limited companies
- **HMRC Approvals** – permanently
- **Income Tax / NI Returns / Income Tax Returns / Correspondence with HMRC** – 3 full tax years
- **National Minimum Wage Records** - 3 full tax years
- **Retirement Benefits Schemes** – 6 years from the end of the scheme year in which the event took place.
- **Statutory Maternity Pay records** – 3 years after the end of the tax year in which the maternity period ends.
- **Pay records** – 6 years
- **Money purchase details** – 6 years after transfer or value taken.
- **Pensioners records** – 12 years after benefit ceases
- **Statutory sick pay records** – 6 years after employment ceases
- **Furlough records** – 6 years

Employment records

- **Records relating to children and young adults** – until the person reaches the age of 21
- **Working time records** – 2 years from date on which they were made
- **Recruitment Application forms / Interview Notes (for unsuccessful candidates)** – 1 year
- **Parental leave** – 18 years from the birth of the child
- **Pension scheme investment policies** – 12 years from the ending of any benefit payable under the policy
- **Personnel files and training records** – 6 years after employment ceases
- **Redundancy records** – 6 years from the date of redundancy
- **Senior management records** – permanently
- **Subject Access Request** – 1 year following completion of the request
- **Trade union agreements** – 10 years after ceasing to be effective
- **Works council minutes** – permanently
- **Whistleblowing documents** – 6 months following the outcome
- **References** – 1 year after the reference is given
- **Right to work in UK Checks** – 2 years after employment ends