

POLICY BRIEF & PURPOSE

This policy sets out how Manchett processes the personal data of data subjects, including the personal data of job applicants and the personal data of our current and former directors, employees, workers, agency workers, apprentices, interns, volunteers, contractors, consultants, clients, customers, suppliers and other third parties. It applies to all personal data that we process, regardless of the media on which those personal data are stored, e.g., electronically, on paper or on other materials.

SCOPE

This policy applies to all members of staff and customers/clients of Manchett. It is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services. Under the data protection legislation, the transparency principle requires the Company to provide specific information to data subjects through appropriate privacy notices.

POLICY ELEMENTS

This Policy has been update in light of the new **Data Protection Act 2018 (DPA 2018) and GDPR Act 2018.**

The Company is committed to being clear and transparent about how we collect and use personal data and to complying with our data protection obligations. Protecting the confidentiality, security and integrity of the personal data that we process is also of paramount importance to our business operations.

The Company will process personal data relating to you in accordance with this policy, the data protection legislation and the latest privacy notice which has been issued to you. This includes:

- The identity and contact details of the Company (as data controller) and any representative
- Where applicable, the identity and contact details of the data protection officer
- The purposes for which the personal data will be processed
- The lawful basis or bases for processing
- Where we are relying on our legitimate interests (or those of a third party) as the lawful basis for processing, what those legitimate interests are
- The categories of personal data, unless they were obtained directly from the data subject
- The third-party sources that the personal data originate from, unless they were obtained directly from the data subject
- The recipients, or categories of recipients, with whom the personal data may be shared
- Details of transfers to non-EEA countries and the suitable safeguards applied
- The retention period for the personal data or, if that is not possible, the criteria to be used to determine the retention period
- The existence of the data subject's rights, i.e. Subject access, rectification, erasure, restriction of processing, objection and data portability
- The right to withdraw consent to processing at any time, where consent is being relied on as the lawful basis for processing
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation, or a requirement necessary to enter into a contract, and the possible consequences of failing to provide the personal data
- The existence of any automated decision-making, including profiling, and meaningful information about how decisions are made, the significance and consequences.

Such information may be kept in either computer or manual records. In processing such personal data Manchett will comply with the data protection principles within the **Data Protection Act 1998**.

The data protection legislation also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies (this is an additional requirement; the processing must still meet one or more of the conditions for processing set out above). These include where:

- The data subject has given their explicit consent to the processing of their personal data for one or more specified purposes; explicit consent requires a very clear and positive statement and it cannot be implied from the data subject's actions
- The processing is necessary for the purposes of carrying out obligations or exercising specific rights of either the company or the data subject under employment law or social security law
- In the case of special categories of personal data, the processing relates to personal data which are manifestly made public by the data subject
- The processing is necessary for the establishment, exercise or defence of legal claims

DATA PROTECTION RESPONSIBILITIES - OVERALL RESPONSIBILITIES

Manchett permit the companies staff to use computers and relevant filing systems (manual records) in connection with their duties. The Directors have legal responsibility for the notification process and compliance of the **Data Protection Act 1998**. The Directors responsibilities include:

- Ensuring that the policy is produced and kept up to date
- Ensuring that the appropriate practice and procedures are adopted and followed by Manchett staff
- Ensure data protection is maintained and renewed annually for all use of personal identifiable information
- Ensure compliance with individual rights, including subject access requests
- Act as a central point of contact on data protection issues within the company

All line managers across the company are directly responsible for:

- Ensuring their staff are made aware of this policy and any notices
- Ensuring their staff are aware of their data protection responsibilities
- Ensuring their staff receive suitable data protection training
- Ensuring customer details remain confidential

RETENTION: MEMBERS OF STAFF

The Company will generally hold personal data, including special categories of personal data and criminal records personal data, for the duration of a member of staff's employment or engagement. The exceptions are:

- Any personal data supplied as part of the recruitment process will not be retained if they have no bearing on the ongoing working relationship
- Criminal records personal data collected in the course of the recruitment process will be deleted once they have been verified through a DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by the company as relevant to the ongoing working relationship
- It will only be recorded whether DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by the company as relevant to the ongoing working relationship
- If it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after [six months] or once the conviction is "spent" if earlier (unless information about spent convictions may be retained because the role is an excluded occupation or profession)

- Disciplinary, grievance and capability records will only be retained until the expiry of any warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment).

STORAGE LIMITATION

Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

The Company will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements.

This includes special categories of personal data and criminal records personal data. You must comply with the Company's rules on data retention and destruction set out below.

GENERAL RESPONSIBILITIES

All Manchett employees, including temporary and contract staff are subject to compliance with this policy.

Under the GDPR individuals can be held personally liable for data protection breaches.

All Manchett employees have a responsibility to inform the company of any new use of personal data, as soon as reasonably practicable after it has been identified.

All Manchett employees will, on receipt of a request from an individual / Company for information held, known as a subject access request or concerns about the processing of personal/company information, immediately notify the Director.

Signed: 

Date: January 2023

Managing Director

Review Date: January 2024