Data protection policy

1. Definitions

(a) **GDPR** means the General Data Protection Regulation.

(b) **Responsible person** means Emma North.

(c) **Register of systems** means a register of all systems or contexts in which personal data is processed by our firm.

2. Data protection principles

We are committed to processing data in accordance with its responsibilities under the GDPR, whose Article 5 "Principles relating to processing of personal data" are outlined below:

Personal data collected will be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date. Reasonable steps are taken to ensure that any inaccuracies are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods, such as for archiving purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR; and

(f) processed 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.

3. General provisions

(a) This policy applies to all personal data processed by our firm.

(b) The responsible person takes responsibility for our ongoing compliance with this policy.

(c) This policy is reviewed annually.

(d) The firm will remain registered with the Information Commissioner's Office as an organisation that processes personal data.

4. Lawful, fair and transparent processing

(a) To ensure our processing of data is lawful, fair and transparent, we maintain a register of systems.

(b) The register of systems is reviewed annually.

(c) Individuals have the right to access their personal data and any such requests made to us will be dealt with in a timely manner.

5. Lawful purposes

(a) All data processed by the firm must be done on a lawful basis. Data is processed by consent, contract, legal obligation, vital interests, public task or legitimate interests.

(b) The appropriate lawful basis is noted in the register of systems.

(c) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent through agreement to our Client Care and Terms of Business will be kept with the personal data.

(d) Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems are in place to ensure such revocation is reflected accurately in the firm's systems.

6. Data minimisation

We ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7. Accuracy

(a) We take reasonable steps to ensure personal data is accurate.

(b) Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8. Archiving/removal of personal data

(a) To ensure that personal data is kept for no longer than necessary, we have a file retention policy for each area in which personal data is processed and review this process annually.

(b) The file retention policy considers what data should be retained, for how long, and why, including requirements stipulated by the Solicitor's Regulation Authority and legislation.

9. Security

(a) We ensure that personal data is stored securely using modern software that is kept up to date.

(b) Access to personal data is limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information.

(c) When personal data is deleted this is done safely such that the data is irrecoverable.

(d) Appropriate back-up and disaster recovery solutions are in place.

10. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we will promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Information Commissioner's Office. More information about this is available on the website: https://ico.org.uk/.