Data Protection Policy

Introduction
General Data Protection Regulation (GDPR) governs the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data to carry on our work. This personal information will be collected and dealt with appropriately.

The Company MD will be the data controller for the information held. Staff who have access to personal information will comply with this policy.

Purpose of this Policy
The purpose of this policy is to set out the Company commitment and procedures for protecting personal data.

GDPR
This contains six principles for processing personal data with which the Company must comply.

Personal data is processed:

- Lawfully, fairly, and in a transparent manner
- For specified, explicit, and legitimate purposes
- Adequately, relevant and limited to what is necessary
- Accurately and kept up-to-date
- And kept in a form which allows identification of individuals for only as long as is necessary
- Securely by implementing appropriate technical and organisational measures.

Implementation
The Company MD is responsible for ensuring that the policy is implemented and has overall responsibility to ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained
- Everyone processing personal information is appropriately supervised
- Those wanting to make enquiries about handling personal information know what to do
- Anybody representing the Company deals promptly and courteously with enquiries about the handling of personal information
- The Company describes clearly how it handles personal information
- The Company regularly reviews and audits the ways in which it holds, manages and uses personal information
- The Company regularly assesses and evaluates its methods and performance in relation to handling personal information.

Risk management
The consequences of breaching GDPR can cause harm or distress to individuals if their information is released to inappropriate people. Staff are made aware that they can be personally liable if they use freelancer or customers' personal data inappropriately.

Data collection: Informed consent
When collecting data, we will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for
- Grants consent.

Rights of data subjects
Individuals have the following rights under GDRP:

- The right of access to their own personal data
- The right to have information erased
- The right to to have inaccuracies corrected
- The right to object to, or to restrict processing.

Procedures for handling data & data security
The Company has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

All staff must therefore ensure that personal data is dealt with properly, no matter how it is collected, recorded or used.

Personal data relates to data of living individuals who can be identified from that data and when use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data. However, combining various data elements such as a person's name and salary etc. would be classed as personal data and falls within the scope of GDPR.

Data storage
Information and records relating to staff, freelancers and clients is stored securely and only accessed by the MD and directly authorised staff with passwords. There is a monthly procedure for checking for out of date personal data and disposal. Personal data is stored only for as long as it is needed or required by law and will be disposed of appropriately by shredding. It is our responsibility to ensure that all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Minimising risk
This policy is designed to minimise the risks and to ensure that the reputation of the Company is not damaged through inappropriate or unauthorised access and sharing.