DATA PROTECTION POLICY

A) INTRODUCTION

We may have to collect and use information about people with whom we work. These may include members, current, past and prospective employees, clients, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us. It covers our response to any data breach and other rights under GDPR.

This policy applies to the personal data of customers and clients, job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1) **The principles of data protection**
The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

The Principles require that personal information:

a) shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

b) shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

c) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

d) shall be accurate and where necessary, kept up to date;

e) shall not be kept for longer than is necessary for that purpose or those purposes;

f) shall be processed in accordance with the rights of data subjects under the Act;

g) shall be kept secure i.e. protected by an appropriate degree of security;

h) shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **"sensitive" personal data**.

Personal data is defined as data relating to a living individual who can be identified from:

a) that data;

b) that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

a) racial or ethnic origin;

b) religion or other beliefs;

c) trade union membership;

d) physical or mental health or condition;

e) sexual life;

f) criminal proceedings or convictions.

2) **Handling of personal/sensitive information**

We will, through appropriate management and the use of strict criteria and controls:

a) observe fully conditions regarding the fair collection and use of personal information;

b) meet our legal obligations to specify the purpose for which information is used;

c) collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

d) ensure the quality of information used;

e) apply strict checks to determine the length of time information is held;

f) shall be accurate and where necessary, kept up to date;

g) shall not be kept for longer than is necessary for that purpose or those purposes;

h) shall be processed in accordance with the rights of data subjects under the Act;

i) shall be kept secure i.e. protected by an appropriate degree of security;

In addition, we will ensure that:

a) everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

b) methods of handling personal information are regularly assessed and evaluated;

All members of staff are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff must take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

a) paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

b) personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;

c) individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or directors must:

a) ensure that they and all of their staff who have access to personal data held or processed for or on behalf of us, are aware of this policy and are fully aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Company and that individual, company, partner or firm;

b) allow data protection audits by us of data held on our behalf (if requested);

c) indemnify us against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by us will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by us.

3) **Implementation**

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.