# 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.

## B) 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.

## C) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) Processing will be fair, lawful and transparent
b) Data can be collected for specific, explicit, and legitimate purposes
c) Data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) Data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) Data is not kept for longer than is necessary for its given purpose
f) Data will be processed in a manner that ensure appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) We will comply with the relevant GDPR procedures for international transferring of personal data

## D) RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed a Data Protection Officer (Kat Titterrell, Operations Manager) who is responsible for reviewing and auditing our data protection systems.

## E) LAWFUL BASES OF PROCESSING

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the individual's consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Individuals will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

## F) ACCESS TO DATA

As stated above, individuals have the right to access the personal data that we hold on them. To exercise this right, individuals should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive or unless a request is made for duplicate copies to be provided to parties other than the individual making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request Policy.

## G) DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that they are only accessed by people who have a need and right to access then and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

## H) INTERNATIONAL DATA

The Company does not transfer personal data to any recipients outside of the EEA.

## I) REQUIREMENT TO NORIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available on our Breach Notification Policy.

## J) RECORDS

The Company keep records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

## K) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Kat Titterrell
kat.titterrell@wisebuddah.com
Operations Manager