**Procedure**

The Company holds personal data about job applicants, past or present employees, clients, suppliers and other individuals for a variety of business purposes, for example personnel, administrative, financial, regulatory, payroll and business development purposes and health and safety.

This policy sets out how the Company seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work.

This policy requires staff to ensure that the Compliance Officer is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

**Scope**

This policy applies to all staff, which for these purposes includes employees, apprentices, volunteers, placement students, temporary and agency workers and other contractors.

**Definitions**

In this policy:

“Personal Data” means information relating to an individual who can be directly or indirectly identified from that data alone or in combination with other identifiers the Company possesses or can reasonably access. Personal data can be factual (for example, a name, email, address, location or date of birth) or an opinion about that person’s actions for behaviour.

“Special Categories of Personal Data” means information 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).

“Data Processing” means any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

**Data protection principles**

The Company’s policy is to process personal data in accordance with the applicable data protection laws and rights of individuals.

The Company will observe the following principles in respect of Data Processing which require Personal Data to be:

Processed fairly, lawfully and in a transparent manner;

Collected for specific, explicit, and legitimate purposes;

Adequate, relevant and limited to what is necessary for the purposes for which the data is processed;

Accurate and where necessary kept up to date~~.~~;

Not kept in a form which permits identification for longer than is necessary for its given purpose;

Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss, destruction or damage;

Not transferred to another country without appropriate safeguards in place; and

Made available to individuals and allow them to exercise certain rights in relation to their Personal Data.

**Fair and lawful processing**

Staff should generally not process Personal Data unless:

the individual whose details are being processed has consent to this;

the processing is necessary to perform the Company’s legal obligations or exercise legal rights; or

the processing is otherwise in the Company’s legitimate interests and does not unduly prejudice the individual’s privacy.

When gathering Personal Data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the Compliance Officer.

It will normally be necessary to have an individual’s explicit consent to process Special Categories of Personal Data unless exceptional circumstances apply or the processing is necessary to comply with a legal requirement. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the Compliance Officer for more information on obtaining consent to process Special Categories of Personal Data.

**Accuracy, adequacy, relevance and proportionality**

Staff should make sure data processed by them is accurate, adequate, relevant, and proportionate for the purpose for which it was obtained. Personal Data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask the Company to correct Personal Data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the Personal Data held is accurate, they should nevertheless record the fact that it is disputed and inform the Compliance Officer.

Staff must ensure that Personal Data held by the Company relating to them is accurate and updated as required. If personal details or circumstances change, the Company’s records should be updated.

**Security**

Staff must keep Personal Data secure against loss or misuse. Personal Data must not be provided to third parties unless it is necessary to do so and in accordance with the data protection principles. Where the Company uses external organisations to process Personal Data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard security of Personal Data. Staff should consult with the Compliance Officer to discuss the necessary

steps to ensure compliance when setting up any new arrangement or altering any existing agreement.

**Data Processing**

Where any Personal Data that the Company holds is passed to third parties to process on our behalf this must only be done where we have satisfied ourselves as to the suitability of such third party and have a formal written agreement in place. All such agreements must be approved by the Compliance Officer.

**Data Retention**

Personal Data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the Personal Data was obtained.

**International Transfer**

Staff should not transfer Personal Data internationally without first consulting the Compliance Officer. There are restrictions on international transfers of Personal Data from the UK to other countries because of the need to ensure adequate safeguards are in place to protect the Personal Data. Staff unsure of what arrangements have been or need to be put in place to address this requirement should contact the Compliance Officer.

**Rights of individuals**

Individuals are entitled (subject to certain exceptions) to request access to information held about them. All such requests should be referred immediately to their Line Manager. This is particularly important because the Company must respond to a valid request within the legally prescribed time limits.

Any member of staff who would like to correct or request information that the Company holds relating to them should contact their Line Manager. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

Staff should not send direct marketing material to someone electronically (e.g. by email) unless they have consented to receiving such communications. Staff should abide by any request from an individual not to use their Personal Data for direct marketing purposes and should notify the Compliance Officer about any such request. Staff should contact the Compliance Officer for advice on direct marketing before starting any new direct marketing activity.

**Reporting breaches**

Staff have an obligation to immediately report actual or potential data protection compliance failures to the Compliance Officer as soon as they are identified. This allows us to:

investigate the failure and take remedial steps if necessary; and

make any applicable reports to the Information Commissioner and others. We have a very short period of time to make sure reports.

**Training**

We are required to ensure all staff have undergone adequate training to enable them to comply with data privacy laws.

**Records**

We are required to keep full and accurate records of all our data processing activities.

**Consequences of failing to comply**

The Company takes compliance with this policy very seriously, Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

**Further Guidance**

**www.gov.uk/search/all?keywords=gdpr&order=relevance**