DATA PROTECTION POLICY

Summary

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 during their work. We are committed to making our Data Protection Policy compliant with GDPR (the EU's General Data Production Regulation).

The Company holds personal data about job applicants, employees, clients, suppliers, and other individuals for a variety of business purposes.

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 during their work.

This policy requires staff to ensure that the Company's Data Protection Officer should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The Company's Data Protection Officer is currently the Director.
The Company's Data Protection Officer is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments, you should contact them.

Definitions

In this policy:

business purposes	means the purposes for which personal data may be used by the Company, e.g., personnel, administrative, financial, regulatory, payroll and business development purposes;
personal data	means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers, and marketing contacts. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual;
sensitive personal data	means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy;
processing data	means obtaining, recording, holding, or doing anything with it, such as organising, using, altering, retrieving, disclosing, or deleting it.

General principles

The Company's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All employees have personal responsibility for the practical application of the Company's data protection policy.

The Company will observe the following principles in respect of the processing of personal data:

- To process personal data fairly and lawfully in line with individuals' rights.
- To make sure that any personal data processed for a specific purpose are adequate, relevant, and not excessive for that purpose.
- To keep personal data accurate and up to date.
- To keep personal data for no longer than is necessary.
- To keep personal data, secure against loss or misuse.
- Not to transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland, and Liechtenstein) without adequate protection.

Fair and lawful processing

Staff should generally not process personal data unless:

- The individual whose details are being processed has consented 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 Director.

It will normally be necessary to have an individual's explicit consent to process 'sensitive 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.

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 inaccurate, they should nevertheless record the fact that it is disputed and inform the Office Administrator.

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, staff should inform the Office Administrator so the Company's records can be updated.

Security

Staff must keep personal data secure against loss or misuse in accordance with the Company's Data Protection Policy.
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 the security of personal data.

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 were obtained.

International transfer

Staff should not transfer personal data without first consulting the Company's Director. 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 Company's Director.

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 the HR department. 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 the Director. The Company may charge a small fee or £10.00 for providing the requested personal data, as permitted by law. 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 there is an existing business relationship with them in relation to the services being marketed. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes. Staff should contact the Company's Director for advice on direct marketing before starting any new direct marketing activity.

Reporting breaches

Staff have an obligation to report actual or potential data protection compliance failures to the HR department. This allows the Company to:

- investigate the failure and take remedial steps if necessary; and
- make any applicable notifications.

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.
Staff with any questions or concerns about anything in this policy should not hesitate to discuss these with the Company's Data Protection Officer.