Data Protection Policy

Statement

The Company will keep certain data about employees for the purpose of running its normal business operations and for managing personnel obligations and issues. Personal data concerning individuals that are not employees that is handled by Company employees will also be protected.
Current legislation provides that this information should be treated in a certain way. This policy is not intended to be a summary of data protection legislation. However personal data should be used in accordance with eight principles of good practice as follows:

- fairly and lawfully processed;
- processed only for those specified purposes notified to the Information Commissioner;
- adequate and relevant and not excessive in relation to the purpose or purposes for which it is processed;
- accurate and where necessary kept up to date;
- kept for no longer than is necessary;
- processed in accordance with the individual's rights. Individuals should be given access to information held about them and where appropriate, incorrect data should be corrected or erased;
- kept securely;
- transferred to no countries where adequate data protection measures are not in force.

Protected Data

Data that is protected is known as either "personal data" or "sensitive personal data". Personal data is information from which an individual can be identified (whether from that information or from that information together with other information in or likely to come in to the possession of the Company).
Sensitive personal data is subject to greater protection than personal data. In relation to an individual this will include information concerning religious or similar beliefs, sexual life, political opinions, trade union activities, actual or alleged criminal offences, physical or mental health, or relating to ethnic origins.

Policy

1. Data Protection Obligations

The following rules will be applied by the Company in dealing with protected employee data:

1.1 The Company shall process all personal data in accordance with the eight principles of good practice set out at the beginning of this policy.

1.2 Protected data will only be processed outside the Company in conformity with data protection law.

1.3 All personal data subjects (including permanent employees, temporary employees, workers, job applicants, Candidates and agents) will be provided on request with the name and contact details of the Company's Data Controller.

1.4 The Company's Data Controller is James Gunning

1.5 No protected data will be processed in, or disclosed or transferred to any country outside the European Economic Area (or other area permitted by European Union rules) without the consent of the subject of the relevant individual.

1.6 Sensitive personal data will be retained separately from ordinary data;

1.7 All protected data, whether held electronically, in manual systems or by any other means will be subject to regular checks and review procedures to ensure its accuracy and whether the data continues to be required for the specified or legal purposes for which it is held.

1.8 All computerised protected data files will be subject to and secured by a password system.

1.9 All manual filing systems containing protected data relating to employees (temporary, permanent or other) whether past or present will be kept in secured filing cabinets and may only be accessed or altered by the Personnel Manager and Directors of the Company.

1.10 All protected data which is no longer required by the Company and will not be required for any legitimate reason by the authorities will be destroyed.

1.11 Company employees will receive training in relation to the lawful processing of personal data and sensitive personal data.

2. Employee Obligations in Processing Protected Data

2.1 It will be a disciplinary offence for any employee to breach this policy (this applies whether the data relates to an employee or other third party [such as a job seeker or Candidate] in dealing with protected data held by the Company). In the most serious cases this may entitle the Company to terminate an employee's contract of employment.

2.2 Protected data should be kept securely and should be protected from any loss, damage or disclosure. The following obligations apply to all employees:

2.3 Employees are responsible for any protected data that they may hold, control, process or have access to and should take all precautions to prevent any unauthorised loss, alteration or access to it.

2.4 Employees should abide by all additional Company rules notified to them and applying to protected data and its security.

2.5 Protected data may only be used for the legitimate purposes of the Company and may not be communicated, by any means, to any other person (whether or not an employee) unless that communication is necessary and for such purposes and is properly authorised.

2.6 Protected data may only be provided to persons outside of the Company (for example for references or to the authorities) with specific written authorisation from Immediate Managers or other senior Company manager.

2.7 The eight principles of good practice referred to above under the section entitled "Policy Statement" apply to all employees.

2.8 Files or information containing protected data should not be left unattended on computer screens or otherwise accessible to any unauthorised person.

2.9 Only specifically authorised employees may process personal data and/or sensitive personal data and in the event of any doubt, employees should consult their Immediate Manager as to whether any action is permissible or not.

3. Employee Obligations in Relation to Their Own Protected Data

Employees should follow certain obligations in relation to information that they supply to the Company, or that is already held by the Company, about themselves. Each employee should:

3.1 Ensure that all personal data and all sensitive personal data supplied to the Company by or on behalf of the employee is full, accurate and up to date.

3.2 Immediately inform the Company of any change in any details about the employee that relates to protected data.

3.3 Check and promptly inform the Company of any necessary amendments to any information about the employee held by the Company and disclosed to the employee for any reason.

4. Employee Right of Access to Protected Data Held by the Company

For the purposes of personnel management the Company holds protected data relating to all employees. Frequently, but not in every case, an employee will be entitled to see protected data that relates to him or her.

4.1 The procedure for an employee to obtain related protected data is by applying in writing to the Company's Data Controller for access to all personal data and sensitive personal data held by the Company.

4.2 Within 40 days of receipt of the request the employee will be informed as to why the Company is not obliged to disclose any particular data and/or the employee will be provided with copies of the relevant data that the Company is bound to supply.

4.3 In addition to the provision of any information the Company is obliged to supply, the employee will be informed of the source of any information not provided by employee to the Company (unless the source is clear from the content of the information).

4.4 If the employee does not receive a response to the request from the Company within the 40 days time limit he or she should immediately inform a Director of the Company in writing.

4.5 Should the employee have any objection to the content of the information supplied in relation to the request, or to the way in which the information is being processed by the

Company, a written notice giving full details of any objections should be provided immediately to the Data Controller (if the cause of the employees objections is the source of any damage, loss or distress the employee should also state why and what effect it has had).

4.6 The Company will respond in writing to any notice of objection within 14 days of receipt.

4.7 Please note that the above procedure operates in addition to statutory rights and does not in any way replace those rights.