DAYSPRING
PLACEMENT SOLUTIONS LIMITED

Data Protection Policy

Data Protection Policy Information Pack

June 2020

DATA PROTECTION POLICY

1.0 The policy

It is the Company's policy that personal information is kept secure and disclosed only to those who need to know.

Disclosure occurs whenever information passes from one person to another. It may be written or spoken. Unauthorised disclosure will be treated as a serious offence. Data is protected if it is information which is processed or held on computer or other automated means or is in a manual form and is held as part of a relevant filing system under the Data Protection Act 1998.

2.0 Disclosure within the Company

Within the Company, Managers and other employees should only have access to the personal information they require in order to fulfil the properly authorised requirements of their jobs. Disclosure may be necessary and may properly occur between companies in the group and specified third parties.

The Company is concerned to ensure that it monitors the sex and ethnic mix of employees. Data held about employees will be also be used for equal opportunities monitoring.

2.1 Disclosure to people and organisations outside

As a general rule personal information may only be given to people or organisations outside the Company if the employee (or potential employee, or former employee) has given his consent. Consent may be written or spoken.

3.0 The Data Protection Act 1998

The Data Protection Act 1998 came into force on 1 March 2000. It regulates the use of personal data and, as a 'data controller', the Company is registered under the provisions of the Act and has a legal obligation to ensure that it complies with the principles of the Act. The IT Department holds the Company's registration documents. The scope of the legislation covers the processing of personal data from collection, alteration and distribution, to amendment and deletion.

Personal data includes information from which living individuals can be identified, e.g. names, contact details (including e-mail addresses), video images, voice recordings, photographs and expressions of opinion and/or intention about employees, customers and suppliers. This, of course, includes all of our applicants.

Everyone must make themselves familiar with the Data Protection Principles and the basic rules set out in this policy.

3.1 Subject access to data

The Act grants workers the right to have a copy of the information that an organisation holds about them.

All requests for details on personal data must be made in writing and with a £10 fee. In response, the Company will provide copies of the information held. Please note that there may be circumstances where information cannot be provided because doing so would involve disclosing information on others and it is reasonable to withhold information for these reasons.

Requests from employees will be handled by Head Office. Requests from candidates will be handled in accordance with the Guidelines in the quality procedures. All requests will be dealt with within a reasonable timescale, but no longer than 40 days.

3.2 Overseas transfer of data

The Act forbids transfers of personal data to recipients in countries outside the EU, including transfers in machine-readable forms such as tapes or discs, unless specific conditions are complied with. You must not therefore transmit or carry personal data to countries outside the UK without first satisfying yourself that the transfer is permitted. You are required to refer to your Manager or Head Office in these circumstances before any transfer is made.

3.3 Adequacy, relevance and accuracy

Managers responsible for collections of data containing personal data will review the data regularly to ensure that they are adequate, relevant and accurate. Personal data, which is no longer required, must be deleted or destroyed after 2 years. In many cases it will be appropriate to invite you to check the information held about you and confirm that it is complete and up to date.

4.0 Security

Appropriate measures will be taken to prevent unauthorised access to personal data. Aspects to be considered will include:

(1) physical security of discs, tapes, printouts and manual data

(2) secure siting or locking of computer terminals, personal computers and manual records

(3) password protection and other software controls

Particular care is needed to ensure that security is maintained when data is downloaded to personal computers, and in respect of printouts and derived material supplied to other users. Likewise, where manual records are being updated or changed and earlier versions are discarded. Appropriate care must be taken in all dealings with data covered by the Act.

5.0 Legal penalties

Use or disclosure of personal data outside the terms of a current entry on the Data Protection Register is a criminal offence for which the Company or the individual can be fined.

Contravention of the Data Protection Principles may lead to action by the Data Protection Registrar, who has wide-ranging powers to restrict what personal data the Company is permitted to hold and the ways in which it can use it.

If a data subject suffers damage because of unauthorised use or disclosure, inaccurate or missing data, or the loss or destruction of data he may seek compensation in the courts.

I have read and understood this policy and agree to comply with all of it.

_____

Name

_____

Signature

Date: _____