Addington Ball Recruitment Limited Information Security And Data Protection Policy

As a recruitment company Addington Ball Recruitment Limited (ABR) processes personal data in relation to its own staff, work-seekers and individual client contacts. It is vitally important that we abide by the principles of the Data Protection Act 1998 set out below.

ABR holds data on individuals for the following general purposes:
• Staff Administration
• Advertising, marketing and public relations
• Accounts and records
• Administration and processing of work-seekers personal data for the purposes of work-finding services

The Data Protection Act 1998 requires ABR as data controller to process data in accordance with the principles of data protection. These require that data shall be: -

1. Fairly and lawfully processed
2 Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept longer than necessary
6. Processed in accordance with the data subjects rights
7. Kept securely
8. Not transferred to countries outside the European Economic Area without adequate protection.

Personal data means data, which relates to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of, ABR.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data, which does not amount to processing. It applies to any processing that is carried out on computer including any type of computer however described, main frame, desktop, laptop, palm top etc.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and those people listed in the appendix shall be responsible for doing this.

Data may only be processed with the consent of the person whose data is held. Therefore if they have not consented to their personal details being passed to a third party this may constitute a breach of the Data Protection Act 1998. By instructing ABR to look for work and providing us with personal data contained in a CV work-seekers will be giving their consent to processing their details for work-finding purposes. If you intend to use their data for any other purpose you must obtain their specific consent.

However caution should be exercised before forwarding personal details of any of the individuals on which data is held to any third party such as past, current or prospective employers; suppliers; customers and clients; persons making an enquiry or complaint and any other third party.
Data in respect of the following is “sensitive personal data” and any information held on any of these matters MUST not be passed on to any third party without the express written consent of the individual:

• Any offence committed or alleged to be committed by them
• Proceedings in relation to any offence and any sentence passed
• Physical or mental health or condition•
• Racial or ethnic origins
• Sexual life
• Political opinions
• Religious beliefs or beliefs of a similar nature Whether someone is a member of a trade union

From a security point of view, only those staff listed in the appendix should be permitted to add, amend or delete data from the database. However all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date. In addition all employees should ensure that adequate security measures are in place. For example:

• Computer screens should not be left open by individuals who have access to personal data
• Passwords should not be disclosed
• Email should be used with care
• Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason
• Personnel files should always be locked away when not in use and when in use should not be left unattended
• Any breaches of security should be treated as a disciplinary issue
• Care should be taken when sending personal data in internal or external mail
• Destroying or disposing of personal data counts as processing. Therefore care should be taken in the disposal of any personal data to ensure that it is appropriate. For example, it would have been more appropriate to shred sensitive data than merely to dispose of it in the dustbin.