4exMilitary Jobs Ltd

Information Security and Data Protection Policy

This is the Information Security and Data Protection Policy Statement of 4exMilitary Jobs Ltd trading as "4exMilitary".

As a recruitment company and internet job board, 4exMilitary Jobs Ltd (The Company) processes personal data in relation to its 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.

The Company 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 The Company 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 held longer than necessary
6. Processed in accordance with the data subjects rights
7. Secure
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 the Company.

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. All activity involving data amounts to processing.

It applies to any processing that is performed by the Company, including any type of computer however described, main frame, desktop, laptop, palm top etc.

Data should be reviewed on a regular basis to ensure it is accurate, relevant and up to date and those people listed in the appendix will be responsible for 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 the Company to look for work and providing 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, prior to use.

However caution must be exercised before forwarding personal details of any 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.

Data in respect of the following is “sensitive personal data” information held on any of these matters MUST not be passed 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
- Race or ethnic origins
- Sexual orientations
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Whether a member of a trade union

From a security point of view, only those staff listed in the appendix will 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 must not be left open by individuals who have access to personal data
- Passwords must not be disclosed
- Email must be used with care
- Personnel files and other personal data must 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 must 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.

It should be noted that the incorrect processing of personal data e.g. sending an individual's details to the wrong person; allowing unauthorised persons access to personal data; or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/or negligence leading to a claim against a member Company of The rpc Group of Companies for damages from an employee, work-seeker or client contact. Failure to observe the contents of this policy will be treated as a disciplinary offence.

Data subjects, i.e. those on whom personal data is held, are entitled to obtain access to their data on request and after payment of a fee. All requests to access data by data subjects i.e. staff, members, clients, candidates etc should be referred to David Beck, Managing Director.

Any requests for access to a reference given by a third party must be referred to David Beck, Managing Director and should be treated with caution even if the reference was given in relation to the individual making the request. This is due to the person writing the reference also has a right to have their personal details treated in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore when taking up references an individual must always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference. However if they do not consent then consideration should be given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so the reference may be disclosed in an anonymised form.

Finally it should be remembered that all individuals have the following rights under the Human Rights Act 1998 and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life [Article 8]
- Freedom of thought, conscience and religion [Article 9]
- Freedom of expression [Article 10]
- Freedom of assembly and association [Article 11]
- Freedom from discrimination [Article 14]

David Beck
Managing Director
July 2010

APPENDIX

David Beck – Managing Director
Anita Searle – Company Secretary
Jill Bennett – Office and Accounts Manager
Sarah Ryder – Client Services Administrator
Mike Stride – Senior Consultant
Simon Hawes – Recruitment Consultant