First Recruitment Services

POLICY ON INFORMATION, SECURITY & DATA PROTECTION

As a recruitment company, First Recruitment is a data controller**.** This means it processes personal data about its work seekers, individual client contacts and about its own staff. First Recruitment abides by the eight principles of the Data Protection Act 1998 ("DPA") set out below.

First Recruitment collects, stores and processes personal data on individuals for the following general purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- The administration required for the introduction of temporary and work seekers to its clients

This policy has been approved by the Board of First Recruitment and sets out its rules on data protection and how it deals with the eight data protection principles contained in the DPA involved.

This policy is published by First Recruitment for the benefit of work seekers, individual client contacts and its own staff. Although this policy is not part of the contracts of employment First Recruitment has with its staff, it is a condition of employment that employees who obtain, handle, process, transport and store personal data on its behalf will adhere to the rules of this policy. Any breach of the policy will be taken seriously and may result in disciplinary action against employees, or the cancellation of contracts for suppliers.

Any employee who considers that the policy is not being followed in respect of themselves should first raise the matter with a director of First Recruitment.

A. Definitions of Data Protection Terms

DPA	The Data Protection Act 1998.
Data	Is recorded information whether stored electronically, on a computer or on certain paper-based filing systems
Data subjects	This includes all living individuals about whom First Recruitment holds personal data. A data subject need not be a UK national or resident. All data

	subjects have legal rights in relation to their personal data.
Personal data	Means data relating to a living individual who can be identified from data and other information held by First Recruitment. It does not include mere mention of someone's name in a document.
Data controller	First Recruitment is the data controller of all personal data used in its business.
Data users	Include employees whose work involves using personal data.
Processing	Any activity that involves use of the data.
Sensitive personal data	Includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about the commission of, or any proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings, or the sentence of any Court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

B. The Eight Principles of Good Practice

The DPA requires First Recruitment, as data controller to process data in accordance with the eight principles of good practice set out under the DPA**.** These provide that personal data must be:

1. Processed fairly and lawfully
2. Processed for limited purposes and in an appropriate way
3. Adequate, relevant and not excessive for the purpose
4. Accurate
5. Not kept longer than necessary for the purpose
6. Processed in line with the data subjects' rights
7. Secure
8. Not transferred to people or organisations situated in countries without adequate data protection laws.

In more detail

Fair and lawful processing:

The DPA is not intended to prevent the processing of personal data but to ensure that such processing is done fairly and in accordance with the rights of the data subject. The data subject must be told the identity of the data controller (in this case First Recruitment) and the Compliance Manager, the purpose for which the data is to be processed by First Recruitment and the identity of anyone to whom the data may be disclosed for transfer.

For personal data to be processed lawfully, certain specific conditions must be met. These include a requirement that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed, When sensitive personal data is being processed, additional conditions must be met. For example, that the data subject's explicit consent to the processing of such data will be required.

Processing for limited purposes:

Personal data may only be processed for specific purposes notified to the data subject or for any other purpose specifically permitted by the DPA. Personal data can be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before processing occurs.

Adequate, relevant and non-excessive processing:

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate data:

Personal data must be accurate and kept up to date. Information which is not accurate should be corrected and the data controller will therefore check the accuracy of any personal data at the point of collection and at regular intervals thereafter. Inaccurate or out of date data will be destroyed.

Timely processing:

Personal data should not be kept any longer than is necessary for the purpose for which it is collected. Data will be erased from First Recruitment's systems when it is no longer required.

Processing in line with data subject's rights:

Data must be processed in line with the data subject's rights. Data subjects have a right to:

- Request access to any data held about them by data controller
- Prevent the process of their data for direct marketing purposes
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data security:

First Recruitment will ensure that appropriate security measures are taken against unlawful or authorised processing of personal data and against the accidental loss of or damage to personal data. Data subjects may apply to the Courts for compensation if they have suffered damage from such a loss. First Recruitment will ensure that only those people authorised to use data can access it.

First Recruitment will, in accordance with the DPA, put in place procedures to maintain the security of all personal data from the point of collection to the point of destruction.

Data will not be transferred to people or organisations situated in countries without adequate protection:

Personal data may only be transferred to a third party data processor if it agrees to comply with First Recruitment's procedures and policies, or if it puts in place adequate measures itself. First Recruitment will, in addition, not export personal data to a jurisdiction where the protection is less comprehensive than that offered in the EU.

C. The Implementation of these Principles

When implementing the eight principles of good practice under the DPA, First Recruitment's employees are required to do the following:

- First Recruitment Services staff should be permitted to add, amend or delete data from the database in accordance with their competences and in accordance with our FOJ procedures.
- Computer screens should not be left open by individuals who have access to personal data;
- Passwords protecting personal data should not be disclosed;
- Emails which enclose personal data should be used with care;
- Personal data should be stored in a place in which only any unauthorised attempts to access the personal data may be dealt with. Personal data should not be removed from its usual place in storage without adhering to the principles of this policy;
- Personal data such as personnel files and candidate records should always be locked away when not in use and when in use should not be left unattended;
- Employees should note that destroying or disposing of personal data counts as processing. Therefore care shall be taken in the disposal of personal data to ensure that it is dealt with in an appropriate fashion.
- All employees are reminded that the incorrect processing of personal data may give rise to claims against First Recruitment for breach of contract and/or negligence and/or criminal proceedings. Failure to observe the contents of this policy will therefore be treated as a disciplinary offence.

D. Dealing with Subject Access Requests

Data subjects are entitled to obtain access to the data which First Recruitment holds on their behalf. They do this by requesting access in what is known as a "Subject Access Request".

A Subject Access Request must be made to First Recruitment in writing. Any employee who receives a Subject Access Request should forward it immediately to the Compliance Manager.

Employees are reminded to be careful not to disclose any personal data held by First Recruitment over the telephone. If a request is made for data over the phone and is urgent and cannot be verified in writing, the employee should check the caller's identity to make sure that the information is only given to a person who is entitled to it by asking them, for example, for their birth date or national insurance number.

E. Queries about this Policy

All queries about First Recruitment's Data Protection Act policy on behalf of the data subjects or employees should be addressed in writing to the Directors at Corporate Headquarters, First Recruitment Services Limited, 29 London Road, Bromley, Kent, BN1 1DG.

August 2008