

## **DATA PROTECTION POLICY**

March 2009 Signed: *D.M. Brinkley*  
(for and on behalf Centra Security)

### **1 Introduction:**

The Data Protection Act 1998 and subsequent updates protects employees against the misuse of personal data, and covers both manual and electronic records.

The Act requires that any personal data held should be:

- processed fairly and lawfully;
- obtained and processed only for specified and lawful purposes;
- adequate, relevant and not excessive;
- accurate and kept up to date;
- held securely and for no longer than is necessary; and
- not transferred to a country outside the European Economic Area unless there is an adequate level of data protection in that country.

If you access another employee's records without authority this will be treated as gross misconduct and is a criminal offence under the Data Protection Act 1998, section 55.

### **2 Purposes for Which Personal Data may be Held**

Personal data relating to employees may be collected primarily for the purposes of:

- recruitment, promotion, training, redeployment, and/or career development;
- administration and payment of wages and sick pay;
- calculation of certain benefits including pensions;
- disciplinary or performance management purposes;
- performance review;
- recording of communication with employees and their representatives;
- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and educational courses and/or to assist future potential employers; and
- staffing levels and career planning.

The company considers that the following personal data falls within the categories set out above:

- personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant;
- references and CVs;
- emergency contact details;
- notes on discussions between management and the employee;
- appraisals and documents relating to grievance, discipline, promotion, demotion, or termination of employment;
- training records;
- salary, benefits and bank/building society details; and
- absence and sickness information.

Employees, contractors or potential staff will be advised of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed.

The organisation will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

### **3 Sensitive Personal Data**

Sensitive personal data includes information relating to the following matters:

- the employee's racial or ethnic origin;
- his or her political opinions;
- his or her religious or similar beliefs;
- his or her trade union membership;
- his or her physical or mental health or condition;
- his or her sexual orientation; or
- the commission or alleged commission of any offence by the employee.

### **4 Responsibility for the Processing of Personal Data**

The organisation's Data Controller is the Chief Executive who is responsible for ensuring all personal data is controlled in compliance with the Data Protection Act 1998.

Employees who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Data Controller. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

### **5 Use of Personal Data**

To ensure compliance with the Data Protection Act 1998 and in the interests of privacy, employee confidence and good employee relations, the disclosure and use of information held by the organisation is governed by the following conditions:

- personal data must only be used for one or more of the purposes specified in this Policy;
- Documents may only be used in accordance with the statement within each document stating its intended use; and
- provided that the identification of the individual employees is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g., surveys, staffing level figures); and
- personal data must not be disclosed, either within or outside the organisation, to any unauthorised recipient.

## **6 Personal Data Held for Equal Opportunities Monitoring Purposes**

Where personal data obtained about candidates is to be held for the purpose of Equal Opportunities monitoring, all such data must be made anonymous.

## **7 Disclosure of Personal Data**

Personal data may only be disclosed outside the organisation with the employee's written consent, where disclosure is required by law or where there is immediate danger to the employee's health.

## **8 Accuracy of Personal Data**

The organisation will review personal data regularly to ensure that it is accurate, relevant and up to date.

In order to ensure that our files are accurate and up to date, and so that the organisation is able to contact the employee or, in the case of an emergency, another designated person, employees must notify their line manager or the Chief Executive as soon as possible of any change in their personal details (e.g., change of name, address; telephone number; loss of driving license where relevant; next of kin details, etc).

## **9 Access to Personal Data**

Employees have the right to access personal data held about them. The Company will arrange for the employee to see or hear all personal data held about them within 21 days of receipt of a written request.

## **10 Retention of records.**

The organisation can retain records as recommended by the Information Commissioner in its Employment Practices Data Protection Code.

## **11 Related Policies**

- Confidentiality Policy
- Email and Internet Policy
- Disciplinary Policy
- Equal Opportunities Policy