

DATA PROTECTION AND INFORMATION SECURITY POLICY

As a Recruitment Consultancy, Core-Asset Consulting processes personal data in relation to our staff, candidates and client contacts. It is vitally important that we abide by the principles of the Data Protection Act 1998 set out below.

Core-Asset Consulting holds data for the following key purposes:

- Administration and processing of candidate's personal data for the purpose of job-seeking services
- Accounts and records
- Advertising, marketing and public relations
- Staff administration

The Data Protection Act 1998 requires Core-Asset Consulting 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 information, 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 Core-Asset Consulting.

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.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date and the Directors 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 Core-Asset Consulting to look for work and providing us with personal details contained in a CV candidates will be giving their consent to processing their details for job-seeking 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 a 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 “sensitive personal data” and any 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 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 authorised staff should be permitted to add, amend or delete data from the database. All staff is responsible for notifying the Directors where information is known to be old, inaccurate or out of date. 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 our database
- Passwords should not be disclosed
- Email should be used with care
- Candidate files must be objective and not contain any expression of opinion which may be deemed to be unfair or negative
- 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, please use the nominated waste bins to dispose of CVs or any other information containing personal data, to be shredded
- Ensure that any documents containing personal data including bank details are to be saved in the shared drive in a password protected file.
- Equifax reports should be stored in a password protected file.

It should always be remembered that the incorrect processing of personal data, 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 Core-Asset Consulting for damages from an employee, candidate or client contact. A 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, suppliers; students should be referred to the Directors.



Any request for access to a reference given by a third party must be referred to the Directors and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore when taking references an individual should 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 if they make a subject access request. 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 anonymous 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 express [Article 10]
- Freedom of assembly and association [Article 11]
- Freedom from discrimination [Article 14]

