Data Protection Policy & Guidelines

Introduction

The Data Protection Act 1998 requires every Data Controller who is processing personal data to notify the Information Commissioner unless they are exempt. Failure to notify is a criminal offence.

Organisations and people about which we hold information are referred to in this policy as Golden recruitment compliant staff has been designated as the Data Protection Compliance Officer, the Data Controller for the Golden Recruitment Solutions ltd.

Information we hold

- We hold three types of information which are covered by this policy
  - organisational information – publicly available information about organisations and some confidential information
  - personal information – information about individuals such as names, addresses, job titles
  - sensitive personal information – in general this kind of information is only held about employees. There are, however, instances where sensitive information is held about other people. For example information about dietary requirements at a conference might allow a person's religion to be deduced. Information about organisations is not covered by the Data Protection Act. However there is sometimes ambiguity about whether certain information is personal or organisational.
- We will not hold information about individuals without their knowledge and consent. It is a legal requirement that people know what we are doing with their information and who it will be shared with.
- We will only hold information for specific purposes. We will inform data subjects what those purposes are. We will also inform them if those purposes change.
- If we buy in a mailing list we cannot use it for any other purpose than

the original Data Controller specified – we must check original use.

Access to Information

- We will seek to maintain accurate information by creating ways in which data subjects can update the information held.
- Information about Data Subjects will not be disclosed to other organisations or to individuals who are not members of our organisation, staff or trustees except in circumstances where this is a legal requirement, where there is explicit or implied consent or where information is publicly available elsewhere.
- Data Subjects have the option not to receive marketing mailings from us or other organisations.

- Data Subjects will be entitled to have access to information held about them by us and for what purpose within 40 days or submitting a request.
- Subject to any rules of the organisation awarding the funding, information will not be retained once no longer required for its stated purpose, we will not keep more than a project requires or surplus information 'just in case'. We will establish retention periods and a process to delete personal information when no longer required.
- At the beginning of any new project or type of activity the member of staff managing it will consult the Data Controller about any data protection implications.
- There may be situations where we work in partnership with other organisations on projects which require data sharing. We will clarify which organisation is to be the Data Controller and will ensure that the Data Controller deals correctly with any data which we have collected.

Data Security

- We have procedures for ensuring the security of all electronic personal data. Paper records containing confidential personnel data are disposed of in a secure way. Project documents and staff records are all kept in a

locked filing cabinet, IT equipment containing personal information is kept in a looked room or cupboard when not in use.

- All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep our information secure from would-be thieves. There is no point protecting the personal information we hold with a password if that password is easy to guess.
- We will make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

Our Commitment

- We have a set of procedures covering all areas of our work which we follow to ensure that we achieve the aims set out above.
- We have established a business continuity/disaster recovery plan and we take regular back-ups of computer data files which are stored away from the office at a safe location.
- All new staff will be given training on the data protection policy and procedures. They will be told how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.
- We will carry out an annual review of our data protection policy and procedures.

See also - http://ico.org.uk/for_organisations/sector_guides/charity

Appendix - The Data Protection Principles defined by the Information Commissioners Office (ICO)

Whenever collecting information about people you agrees to apply the Eight Data Protection Principles:

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Data should be accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.