Data Protection Principles

Introduction

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them. The Act works in two ways:

1. it states that anyone who processes personal information must comply with the eight principles
2. it provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

The Eight Principles

State that personal data shall:

1. be collected and processed fairly and lawfully

The purpose for which personal data is collected and processed should be made clear to the data subject. Data subjects should not be deceived or misled as to the purpose for which their personal data is held or used. Personal data should only be obtained from a person who is legally authorised to supply it.

2. be obtained only for the specific and lawful purposes described in the register entry, and shall not be further processed in any manner incompatible with that purpose or those purposes

Personal data held for one purpose should not be used for another, e.g. research data should not be used for direct marketing. All personal data held must be within terms of a register entry or be specifically exempt from registration.

Personal data must not be disclosed to any person not described in the register entry for that data collection. Details of persons to whom data may be disclosed and by whom are contained in the registration. When deciding whether to disclose data Departments should also consider what disclosure procedures were outlined to data subjects when they gave permission for their data to be held. If data subjects have been told that data will only be released with their permission data should not be released without permission, regardless of the register entry.

3. be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are held

All personal data held must be clear in meaning, and convey sufficient information for others to understand them. This is particularly important where specific action is required. Only information that is necessary should be kept. Records should be unambiguous, accurate and professionally worded. Any abbreviations should be widely agreed. Opinions should be clearly distinguishable from matters of fact. Sensitive data must only be held if really necessary.

4. be accurate and, where necessary, be kept up to date

Personal data must not be inaccurate or misleading to any matter of fact. This is equally applicable to information received from a third party. The source of information should always be included on records. Unauthorised abbreviation of names is inaccurate data.

5. be held no longer than is necessary for the registered purpose

The wide range of reasons for the College to hold personal data makes it impossible to lay down absolute rules about how long particular items of personal data should be retained. Failure to remove data when its purpose has been served is a breach of the Act.

6. be processed in accordance with the rights of the data subjects under the Act

Individuals have a statutory right to be told whether information about them is being processed, what the information is, its source, the purposes for which it is going to be processed, to whom it might be disclosed, and the logic involved in any automatic decision process (for example the underlying logic of the computer programme).

The Act also provides that individuals may have access to data held about them and, if appropriate, to have the data corrected or deleted.

If the information is sensitive, individuals must be asked for their explicit consent to the processing of that information.

The Data Controller has a limited right only to make decisions affecting individuals based solely on the automatic decision processing of information about them.

7. be held under secure conditions, together appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Access to personal data must be permitted only for the purposes necessary for the efficient discharge of bona fide duties. The personal or private use of personal data held by the College is strictly forbidden. It is important to consider the sensitivity of the data processed, the locations where data is stored and security measures necessary to hold data securely.

8. not be transferred to a country or territory outside the European Economic Area, unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Personal data must not be transferred to a country outside European Economic Area unless:

- explicit consent has been obtained from the data subject(s)
- the data has been completely anonymised
- that country ensures an adequate level of protection for data subjects
- a contract is in place with the recipient of the personal data, which puts the necessary safeguards in place.