

Data protection Act

The Data Protection Act 1984 was brought about because of the increase in the use of computers, which can store great quantities of personal information and manipulate it easily. It was designed to protect the person on whom the information was kept; by ensuring the information was protected from others who might have an interest in knowing it or using it for an unauthorised purpose. It made no distinction between sensitive or general information – even the person's address was considered confidential. Although the initial act only covered electronic information, the amendments now mean that it covers all information held either on paper or electronic media.

The information held was known as personal data and was defined as being information about living and identifiable people. The medium on which it was held was electronic and was termed automatically processed information. 'Data' is defined as any information in a recorded form. It specifically did not cover written information, but this has now changed.

People who had access to electronic information or who used it in their day-to-day duties were defined as data users and the subjects of the information were defined as data subjects. It is likely that you had to sign a confidentiality clause in your contract meaning that if you disclose confidential information you may be held liable in a court of law. All centres that hold information have to be registered with the Data Protection Registrar. As it may be possible that the information about an individual held on computer or on written records may be incorrect, the individual has the right to see what information is held on them. This is known as subject access right and there will be processes in place in your workplace to enable an individual to access their records. If any information is incorrect or causes distress to the individual, then they can claim compensation. It is important that information on an individual should not be divulged to anyone who doesn't have authority to be a party to that information.

There are eight basic data protection principles, which are that:

- information must be obtained and processed legally
- data should only be held for specific purposes
- personal data held for a purpose should not be disclosed in a manner incompatible with the purpose
- personal data held should be adequate and not excessive
- personal data should be accurate and up to date
- personal data should not be kept longer than necessary
- an individual should have access to their records
- appropriate security measures should protect the data.

There must be strict security surrounding the storage of information. Staff dealing with such information must be aware that it is confidential and that it should not be divulged to anyone not entitled to know it. They should not discuss any information in areas where the information may be overheard. Disclosure of confidential information to an unauthorised person is a criminal offence.

Access to computerised records should be adequately protected. This is usually done with the use of passwords, which should be regularly changed, and restrictions to access. Any changes made to any records should be the subject of an audit trail. This is one reason that you should not use anyone else's password nor allow anyone to use your password to access computer records.