The Data Protection Act 1998 (DPA)

The DPA gives individuals the right to know what information is held about them and also sets out rules to make sure this information is handled properly.

The following principles are set out in the Act for processing both manual data (e.g. written records) and computerised data:

1. Personal data shall be obtained and processed fairly and lawfully
2. Data may only be held for one or more specified and lawful purposes
3. Data must be adequate, relevant and not excessive for the purpose
4. Data must be kept accurate, and if not, must be amended and kept up to date
5. Data must not be kept for longer than necessary
6. Personal data must be processed in accordance with the rights of the data subject
7. Data must be secure and there must be no unauthorised access, alteration, disclosure to third parties or accidental loss
8. Transfer of data outside the European Economic Area is restricted

The right of individuals to see personal information held about them is set out in Section 7 of the Act. This includes written and computerised records held by private companies, employers and public sector organisations such as social work departments, hospitals, doctors and housing departments. There are exemptions which apply to third-party information where the author has refused consent to access (e.g. letters from relatives held in social work files) and where there may be serious risk of harm.

If someone wishes to see their record, they should apply in writing to the relevant organisation. The Act means that if you work in a care or support setting people may ask to access their records. You are under a clear obligation to ensure that what you write (manually or on a computer) is accurate and that any opinions can be justified.

Principle 7 is the most relevant in considering confidentiality and security. This principle should be incorporated into your agency policies and procedures. You should find out what these policies and procedures are so that you do not breach confidentiality. An unjustified breach is a criminal offence liable to a fine of up to £5000. So not only do you show a lack of respect for the service user or carer if you breach confidentiality, you commit an offence and it could be rather costly.

Unlawful disclosure of information can also result from breaches of security, therefore agencies must act responsibly to keep files in locked cabinets, not letting them out of the building except in exceptional agreed circumstances. Workers must also ensure that they do not leave computer records open and visible when unattended, and organisations must ensure that there are secure systems in place for keeping confidential material. This includes systems with secure password access only.

It must be remembered that young people and people with disability usually have the same rights as anyone else in relation to confidentiality. Their parents or other family members do not automatically have the right to see their records or to act on their behalf. Risk is usually the trigger for lawful breaches of confidentiality but as in other instances this must be shown to outweigh the service user's right to confidentiality.

For further information on the Data Protection Act 1998 from ICO (Information Commissioner's Office) visit http://www.ico.gov.uk/what_we_cover/data_protection.aspx