What you need to know about Legislation

Human Rights Act – states that everyone has a right to a private life - protects privacy. So you must treat any personal information you come across by virtue of your job with care.

Data Protection Act 1998 – 8 principles

- It must be collected and used fairly and inside the law
- It must only be held and used for the reasons given to the Information Commissioner.
- It can only be used for those registered purposes and only be disclosed to those people mentioned in the register entry. You cannot give it away or sell it unless you said you would to begin with.
- The information held must be adequate, relevant and not excessive when compared with the purpose stated in the register. So you must have enough detail but not too much for the job that you are doing with the data.
- It must be accurate and be kept up to date. There is a duty to keep it up to date, for example to change an address when people move.
- It must not be kept longer than is necessary for the registered purpose. It is alright to keep information for certain lengths of time but not indefinitely. This rule means that it would be wrong to keep information about past customers longer than a few years at most.
- The information must be kept safe and secure. This includes keeping the information backed up and away from any unauthorised access. It would be wrong to leave personal data open to be viewed by just anyone.
- The files may not be transferred outside of the European Economic Area (that's the EU plus some small European countries) unless the country that the data is being sent to has a suitable data protection law. This part of the DPA has led to some countries passing similar laws to allow computer data centres to be located in their area

Some of these (e.g (6)) have more implications for IT than others

Now superseded by General Data Protection Regulation which tightens up on DPA. People have a right to know what data is held about them and how its used and that its for legitimate reason. The fines for breaking the rules are much greater

The Computer Misuse Act (1990)

This was passed by Parliament and made three new offences:

- accessing computer material without permission, eg looking at someone else's files
- accessing computer material without permission with intent to commit further criminal offences, eg hacking into the bank's computer and wanting to increase the amount in your account
- altering computer data without permission, eg writing a virus to destroy someone else's data, or actually changing the money in an account

Fines and Imprisonment can be given depending on the severity.

PERC
The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Www.ico.org.uk

Some others you should be aware offences
PCIDSS
Copyright
Money Laundering