

Data Protection

Data protection is about protecting people's privacy. This is the purpose of data protection in any organisation, and is at the heart of data protection law, including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Data Protection Principles

Everyone responsible for using personal data must follow strict rules called data protection principles. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

What personal data does the organisation collect, store and use?

Personal data is information about a person which is identifiable as being about them. This includes basic things like names and addresses, and more complex or sensitive information such as ethnicity, criminal record, employment history, sexual orientation, and health information.

Personal data can be held electronically or on paper. Photographic and film images are also considered to be personal data if people are identifiable in them. Further guidance can be found on Community Resource website.

Think about what personal data the organisation holds about people. This is likely to include names and contact details but may also include other more sensitive information.

It is important to understand whether personal data belongs to a group or to an individual. For very small groups this can be a bit confusing. A good rule of thumb is to consider whether members of the group have met a person, or gained their information, during their involvement with the group. If data held about a person belongs to the group and not to individual members of the group, that information should not then be used by individuals for personal reasons without explicit consent.