7 Principles of Data Protection

**Data Protection Principles**

- **Transparency**
  - Identify yourself as the Data Controller in all communications seeking personal data
  - Tell data subjects why you need their data and with whom you’ll share it

- **Data must be obtained & processed fairly**
  - Accountability
    - Be able to demonstrate compliance with each of the obligations under the law

- **Accuracy**
  - Data must be accurate and kept up to date
    - Have accurate data entry
    - Cross check
    - Review data to ensure accuracy
    - Avoid duplication of records

- **Specified & lawful purpose**
  - Purpose Limitation
    - Data is to be only processed for the particular purpose for which it was collected
    - Data can only be processed on a legal basis

- **Adequate, relevant & not excessive**
  - Data Minimisation
    - Only collect the minimum data required for the stated purpose
    - Don’t collect data just because it is available

- **Safe & secure**
  - Integrity & Confidentiality
    - Nature of security will depend upon medium in which data is held
      - Paper: locked cabinets, restricted access to offices, clean desk policy etc.
      - Electronic: Hierarchy of access controls, passwords & logins.
    - Train Staff

- **Retention**
  - Storage Limitation
    - Review the types of data held
    - Have a Retention Policy for each category
    - Dispose of data carefully