Introduction to Data Protection

Community Councils

Legislation

UK GDPR

- The UK General Data Protection Regulation. Following Brexit, the UK GDPR has brought the European GDPR into UK law.

Data Protection Act 2018

- This is the UK Act which replaces the Data Protection Act 1998. It governs the way that organisations collect, use, store and share personal information.

Definitions

Personal Data	• any information that can be used to identify an individual, either on its own or in combination with other data.
Special Category Data	• Race; Ethnicity; Political Opinions; Religious or Philosophical Beliefs; Trade Union Membership; Genetic Data; Biometrics; **Health Data**; Sex Life; Sexual Orientation
Processing	• any action performed on personal data, including collecting, storing, sharing, destroying or preserving data.
Data Subject	• The individual concerned by the data.

Data Controller vs Data Processor
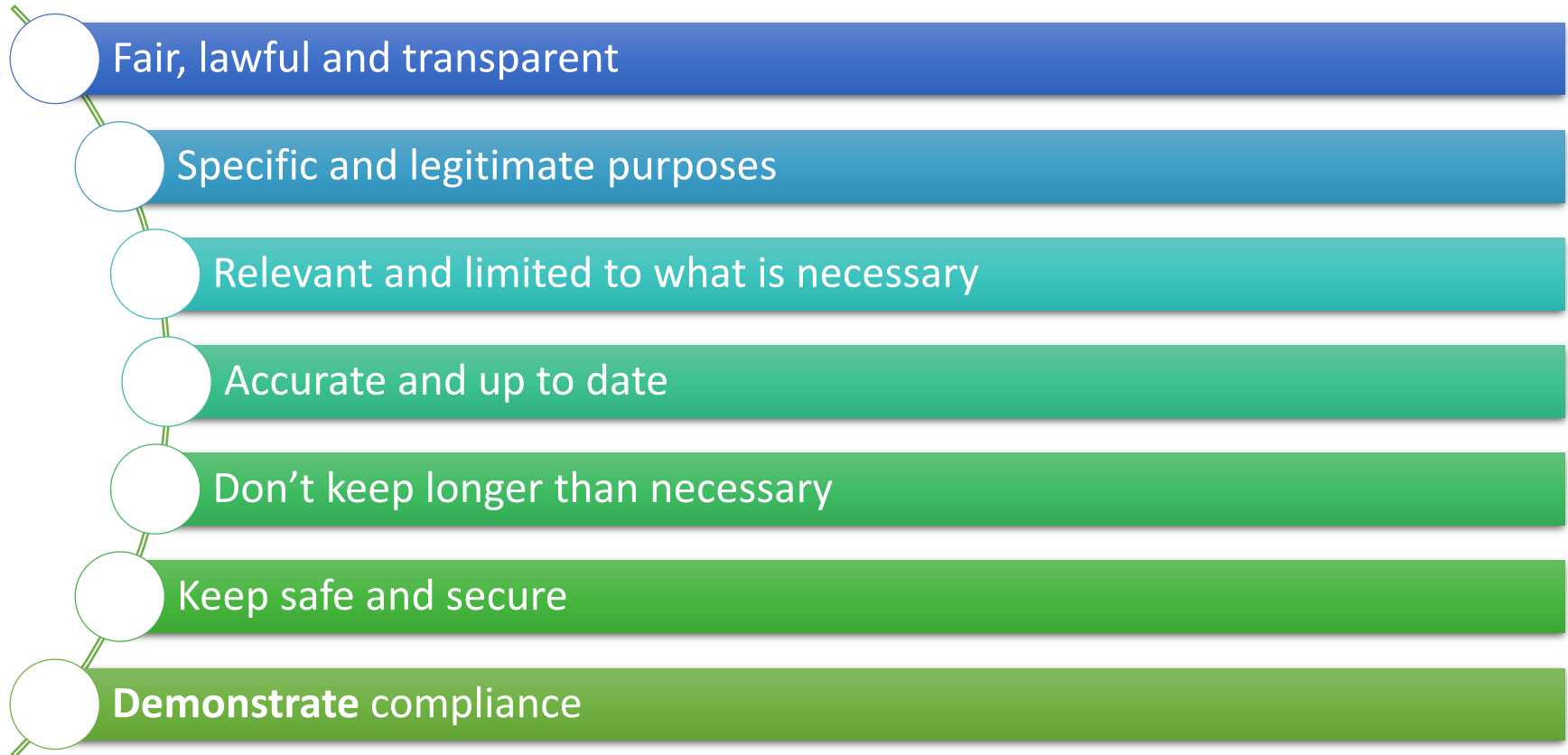
Data Controllers…

- **decide** how and why personal data is collected, stored, used and shared ('means and purposes of processing');
- abide by the **Data Protection Principles;**
- Have specific **obligations** – refer to Guidance and visit https://ico.org.uk for more information.

Data Processors…

- carry out functions on behalf of a Data Controller;
- Abide by any **data sharing arrangements;**
- Undertake relevant **training;**
- Keep data **safe** and secure;
- Abide by the **Data Protection Principles.**

Data Protection Principles

General rule: data processing should be necessary.
If it isn't necessary, it probably isn't compliant!

Fair, lawful and transparent

Specific and legitimate purposes

Relevant and limited to what is necessary

Accurate and up to date

Don't keep longer than necessary

Keep safe and secure

Demonstrate compliance

Data breaches

Breach	Mitigation
Papers sent to wrong address	Build double-checking of names/addresses into procedures.
Emails sent to wrong address	Send test emails to external addresses; use 'Check names' in Outlook;
Papers served to wrong address due to out-of-date information	Perform regular data audits for accuracy.
Discussing medical details over the phone, without confirming identify first.	Always confirm identity before disclosing any personal information.

Examples of Data Breaches

Sending an email to the wrong person

Losing a sheet of paper with personal data

Disclosing personal data unnecessarily

Sharing information without proper protections, e.g. Police

Destroying data inappropriately

Loss or theft of data or equipment on which data is stored

Sending personal data to the wrong address

Information Security

- Housekeeping – don't keep emails forever.
- Save attachments to a shared working area and remove the content from your email.
- Avoid using names and other personally identifiable information when you can.
- Measure twice, cut once – address autocomplete and similar names.
- Never store passwords in your email.
- Remain aware of your environment.
- Use lockable storage to protect paper records.
- Keep copies to a minimum.