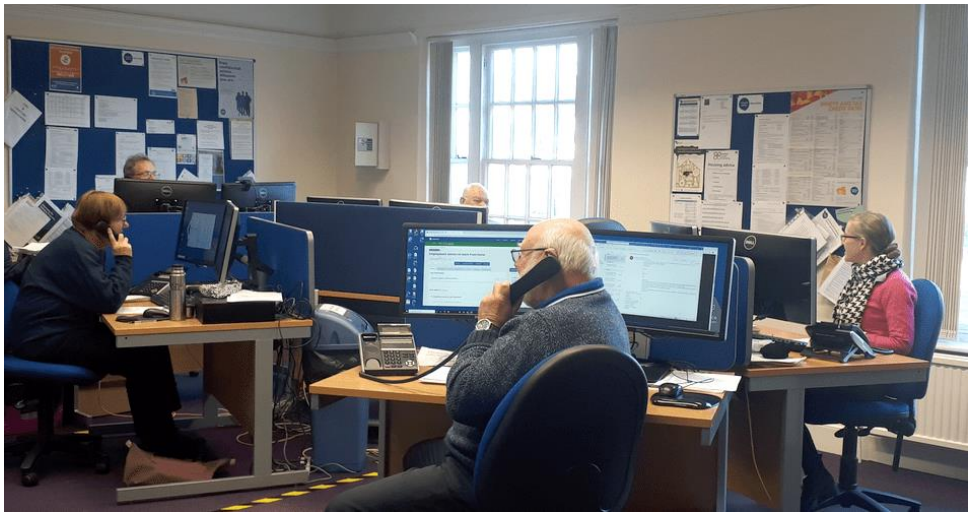
Introduction to data protection

citizens advice Mid Suffolk

Simon Clifton
Chief Officer

Introduction

- Not An expert
- Practitioner of Data Protection in the workplace
- Senior Information Risk Officer for Citizens Advice Mid Suffolk



What is personal data?

- Personal data is information that relates to an identified or identifiable individual
- Personal data only includes information relating to natural persons who:
  - can be identified or who are identifiable, directly from the information in question; or
  - who can be indirectly identified from that information in combination with other information

What is personal data?

There are many common means of identifying an individual that include:

- name;
- identification number;
- location data; and
- an online identifier (Online identifiers' includes IP addresses and cookie identifiers which may be personal data)

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/#

ICO Registration

Who is exempt?

The Information Commissioner's Office Guidance states:

- Organisations which are established for not-for-profit making purposes can be exempt from registration.
- The exemption may therefore be appropriate for small clubs, voluntary organisations and some charities.
- A not-for-profit organisation can make a profit for its own purposes, which are usually charitable or social, but the profit should not be used to enrich others. Any money that is raised should be used for the organisation's own activities.
- Any organisation which is not sure whether or not it is a non-profit making organisation should get appropriate advice, probably from their accountant or legal adviser.

https://ico.org.uk/media/for-organisations/documents/1567/exemption-from-registration-for-not-for-profit-organisations.pdf

Processing & Controlling Personal and Special Category Data

Seven Guiding Principles

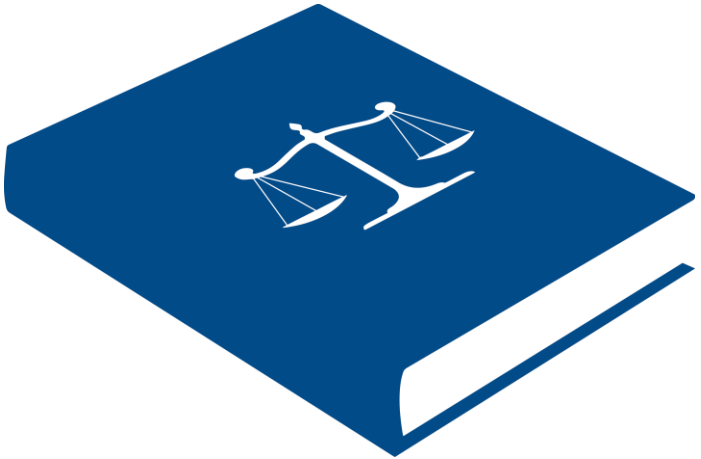
- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Who is responsible for what?

- Accounting Officer (Data Protection Officer)
- Senior Information Risk Officer
- Information Asset Owners

Data Processing and Data Controller

- Data Mapping
- Information Asset Register
- Data Privacy Impact Assessments (DPIA)
- Data Sharing Agreements (DSA)
- Data Processing Agreements (DPA)



Data Protection Policies and Procedures

- Data Protection Policy
- Information Risk Policy
- Data Retention Policy
- Acceptable Use of ICT
- Privacy Policy

Subject Access Requests – Individuals Rights

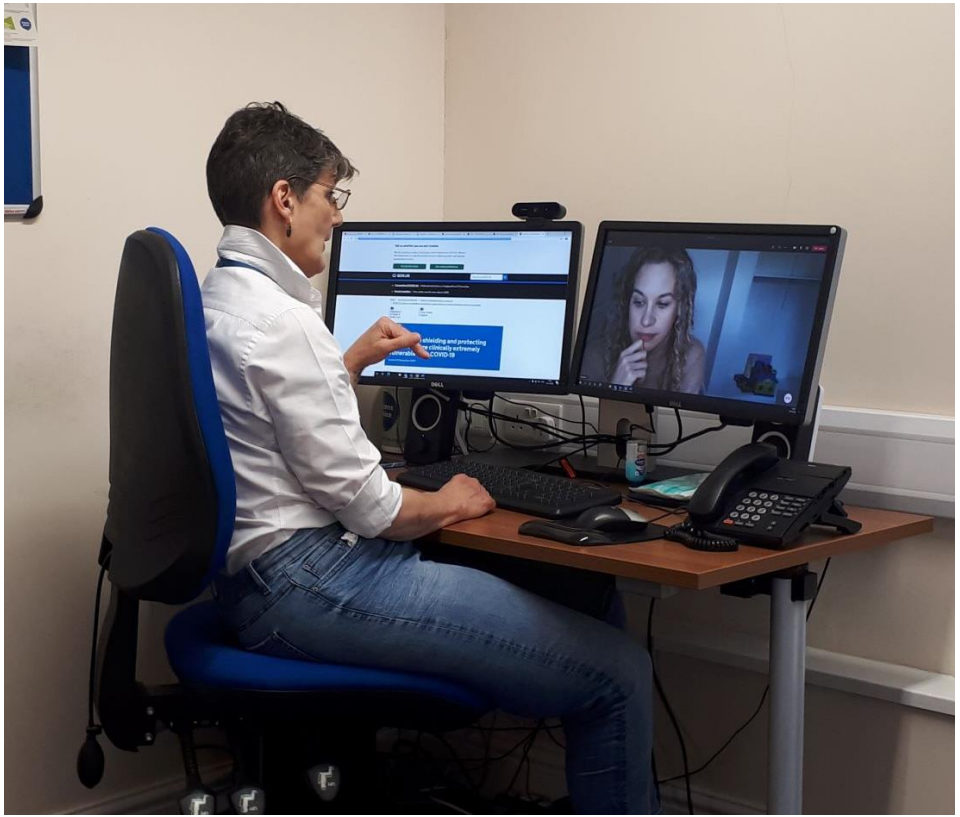
- Individuals have the right to access and receive a copy of their personal data and other supplementary information. This is a Subject Access Request.
- Individuals can make a SAR verbally, in writing and via social media.
- Third parties can in certain circumstances can make a SAR on behalf of another person.

Subject Access Requests – What must you do if you receive a Subject Access Request?

- You must respond without delay and within one month of receipt of the request. This can be extended by a further two months if the request is complex or one of a number of requests by the individual.
- You should perform a reasonable search for the requested information.
- You should provide the information in an accessible, concise and intelligible format.
- The information must be disclosed securely.
- You can only refuse to provide the information if an exception or restriction applies; or if the request is manifestly unfounded or excessive.

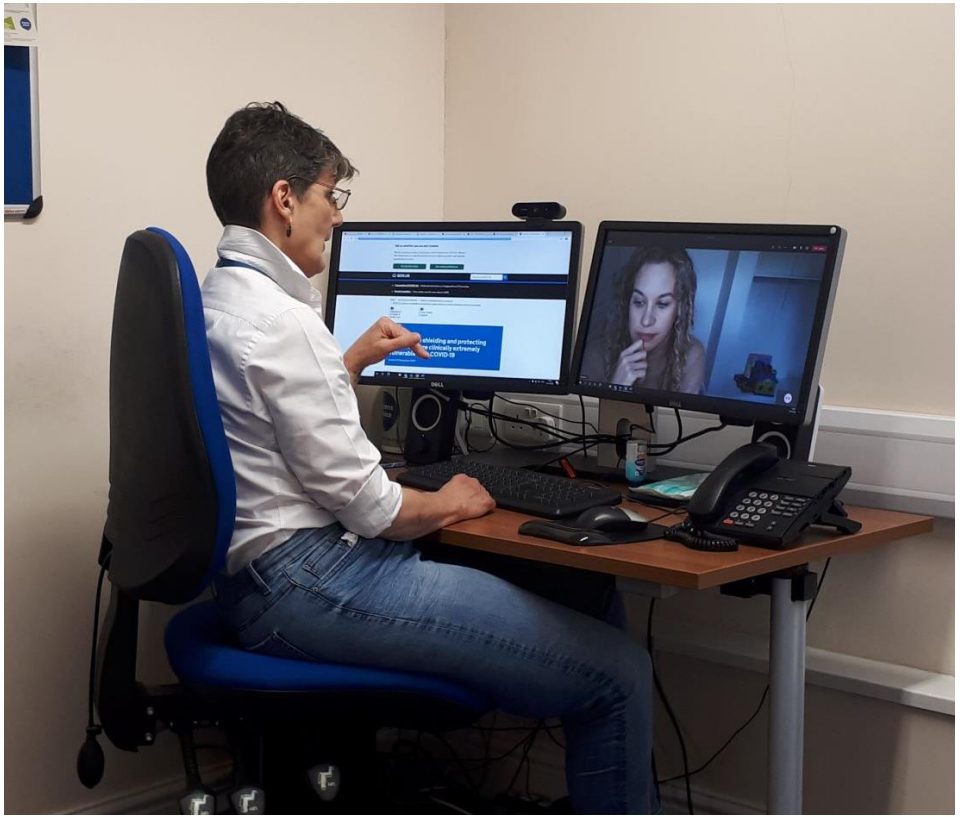
Virtual Advice

- What was the need?
- What did we do?
- What did we learn?
- Where are we now?



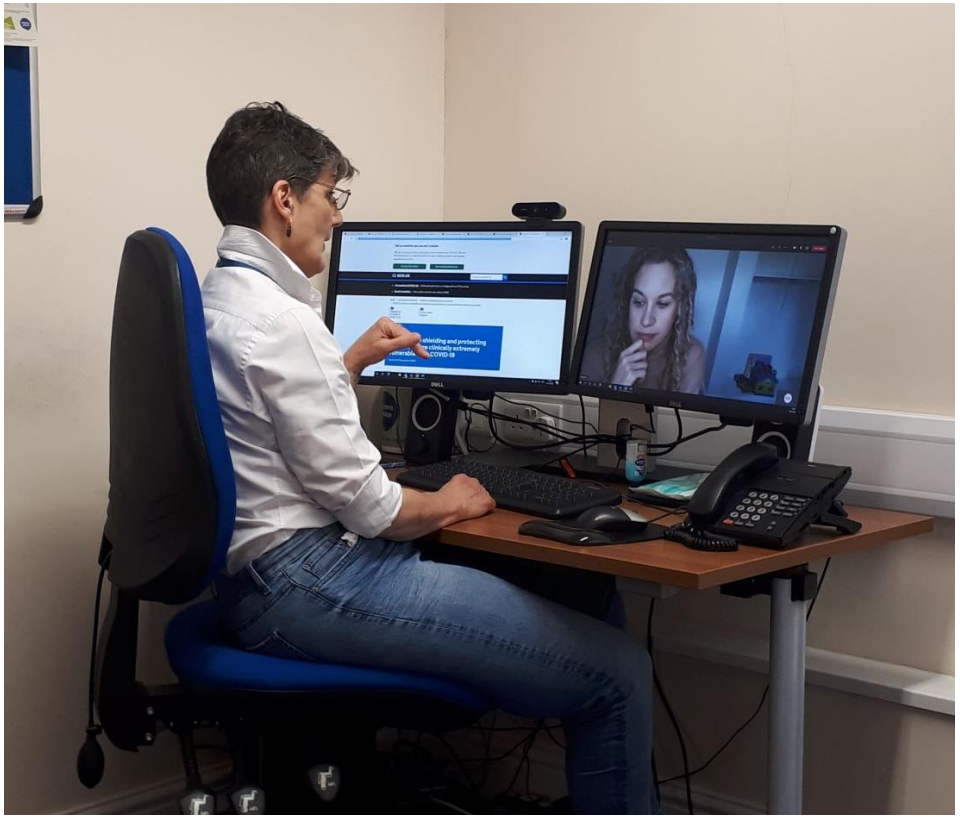
Virtual Advice

What did we do?



Virtual Advice

- What did we learn?
- Where are we now?



Questions?