DEVELOP Promoting Information Security

PUBLISHED 2019.

We all must adhere to the General Data Protection Regulations in our work so it is good to revisit those responsibilities regularly.

Consider what measures you take to protect other people's data, and how you protect your own data too.

DID YOU KNOW

In the government's Cyber Security Breaches Survey 2019, of the businesses questioned 32% had identified breaches or attacks with the most common being;

- Phising E Mails.
- Others impersonating their organisation.
- Viruses and malware.

Businesses reported this took up staff time, and that they needed new systems to defend against these threats. It stopped staff carrying out their daily work and it cost on average £4180 per year when they lost data or assets after breaches (irrispective of any fines imposed by the ICO).

GDPR PRINCIPLES

People should know who is collecting their data and for what purpose.

People should give consent for their data to be used and for what reason.

Organisations should ensure personal data is up to date and accurate.

Organisations must use personal data in a way that is fair.

Organisations should limit data to that which is necessary to meet the task to which people have consented.

Organisations must ensure they have appropriate security measures in place to protect personal data.

Organisations should not keep personal data for longer than they need it.

INFORMATION SECURITY

You should know how to keep information secure within your business so make yourself aware of good security practices and the privacy policies of your own organisation.

It is likely your security policies might include some or all of the following;

- To avoid unnecessary printing.
- To shred confidential waste.
- To password protect sensitive files.
- To avoid saving data to portable devices.
- To never send unencrypted data by e mail.
- To delete unwanted e mails which includes any personal data.
- To use high strength passwords which are never shared.
- To keep storage devices and laptops secure.
- To lock computers when unattended.
- To secure any personal data when unattended.
- To keep desks clear when unattended.
- To double check all requests for personal data.
- To be wary of virus or spam e mails requesting data.

At some level your business will hold data about you too, so hopefully your colleagues will also know how to keep your own data secure.

MANAGING YOUR OWN DATA

Next time you sign up to a product, service or website take a few moments to read the privacy statements or understand where your data will be used.

- You have the right to be informed about the collection and use of your personal data.
- You have the right to access your own personal data.
- You have the right to request that inaccurate or incomplete data is rectified.
- You have an absolute right to stop your data being used for direct marketing.
- You have the right to ask for data to be erased (sometimes known as the right to be forgotten).

You can see more about rights and responsibilities at the Information Commissioner's Office website (ICO).

Act promptly if you think your data is compromised. Change website passwords and security questions immediately. Check all sites have your correct contact details.