

# 10 GDPR 'essentials'



**1** **There must be a unique, complex password for every account.**  
Reusing passwords across different accounts is asking for trouble.

**2** **Always treat other people's personal data as you would have them treat your own.**

**3** **Never, ever leave PCs / Laptops or mobile devices unattended.**  
Please make sure that they are 'locked'.

**4** **Do not hold onto data forever or 'just in case'.**  
Delete data you no longer need.

**5** **Ensure a contract is in place...**  
...with any 3rd party company (e.g. cloud-based CRM) that is processing personal data on behalf of your organisation.

**6** **GDPR is not a 'tick box exercise'.**  
Make sure your data protection policies are clear and easy to understand.

**7** **Mistakes can happen.**  
If you accidentally delete data, lose a company device or send an email to the wrong person, tell your data protection team/lead/officer.

**8** **It's OK to use a cloud-based system to store personal data...**  
...but only if you know 'where' in the world the data is stored and how secure it is.

**9** **Recognise that Data Subjects have the Right to access to data you hold on them.**  
Don't ignore requests; there's only one month to respond.

**10** **Keep your operating system and all software up to date.**  
Where possible enable automatic software updates.