**Dos and Don’ts for Data Protection**

***Do….***

***Take the common sense approach***

1. Review reasons of why you need to keep information.
2. Keep appropriate information – i.e. for a specific reason.
3. For sensitive or confidential electronic data being physically taken off-site or posted - use encrypted devices, such as encrypted USB drives.
4. Keep your business contact list separate from your personal contact list.
5. Save your personal contact list to your phone.



1. Destroy/shred sensitive information when not needed
i.e. medical records, salary information, bank details, credit card details.
2. Protect data held about other individuals in the same way as if it were *your* data.
3. Use ‘strong’ passwords i.e. use a combination of numbers, symbols, uppercase & lowercase letters.



1. Remember, once an email has been sent, you have no control of where it might end up!
Treat it like sending a postcard in the mail!
2. Seek advice from your Data Protection “Champion”, if you are unsure of what to do.
3. Ask third parties how *they* will protect sensitive information, once it has been passed to them.

***Always take the common sense approach!***

**Dos and Don’ts for Data Protection**

***Don’t….***



1. Worry about the complexities of the Data Protection Act.
The basic principles are simple.
2. Give out personal data information without that said person’s *explicit consent*.
3. Write anything in an email that you wouldn’t want your boss to read.
4. Take personal data off site unless encrypted and discussed with IT
5. Don’t leave USB keys containing sensitive information lying around.



1. Walk away from your PC without locking it.
2. Keep information unnecessarily.
3. Put personal information on the website, unless prior permission has been gained first.
4. Hold sensitive data about an individual without the data subject's *explicit consent*.
5. Use data held for one purpose, for a different purpose, without seeking permission to do so.
6. Use public wireless hotspots for access to sensitive information – they are *not* secure.
7. Leave personal information insecure.
8. Refuse Data Subjects access to their personal information.
9. Share your passwords or allow others to access to your user account.
*NB: Authorised IT staff may ask for your password verbally for support purposes, but this is rare.*

***Always take the common sense approach***