Data Protection Dos and Don’ts

DO

- Comply with Data protection principles at all times
- Remember the Act applies to paper files, information held electronically, video/DVD, audiotapes and photographs
- Think of personal data held about individuals as though it were held about you
- Get permission from the data subject to hold their personal data unless consent is obviously implied
- Be particularly careful about sensitive data: concerning race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences
- Hold personal data about people only when necessary
- Do your best to ensure personal data is kept accurate and up to date
- Tell people you hold personal data about them and tell them why you need to do so (fair processing)
- Be open with people about information held about them
- Ensure that you have a contract (data processing agreement) in place when sharing personal data with other organisations
- Be very careful about passing personal data to third parties
- Respect confidentiality and the rights of the data subject
- Review personal data kept in files from time to time and at least annually
- Ensure all personal data is disposed of as confidential waste
- When writing documents, bear in mind that the data subject has a right to see information relating to them
- Realise even deleted emails may be retrieved and revealed to those about whom they are written
- Hold personal data in such a way that it can be collected for inspection at short notice
- Where possible, anonymise personal data for statistical analysis
- Only use software and hardware supported or provided by the College when working with personal data

DON'T

- Worry about the complexities of the Act - the Data Protection Principles are simple
- Reveal personal data to third parties without the data subject's permission or justification (see the College’s guidance on Individual Rights)
- Disclose any personal data over the telephone
- Hold sensitive data about a person without explicit consent
- Put personal data about an individual on the Internet without his/her permission, unless it is a condition of his/her employment or acceptance as a student
- Send personal data outside the European Economic Area (EEA)
- Leave personal data insecure in any way, whether it is physical files or information held electronically
- Take personal data home without particular care for security
- Process personal data on a computer not owned, supplied or approved by the College
- Part with College computers without advice on deletion of data from IT support
- Use email for sending confidential communications or unencrypted personal data, as it is relatively insecure
- Use personal data held for one purpose for a different purpose without permission from the data subject