What is the Data Protection Act 1998 (DPA)? The DPA is a framework for the collection and processing of personal data. Most organisations need to collect and process this kind of information so the services they provide can be delivered effectively to those who are entitled to them.

What is personal information? Broadly speaking, it is any information that identifies a living individual such as name, address, date of birth, educational record, financial details and even expressions of opinions or intentions. The Act covers such information held on computer and paper file.

The Act has eight principles which are key to ensuring the Board stays within this framework while processing personal data. These principles state that personal data must be:

1. processed fairly and lawfully. Personal data should only be collected and used where there is a valid reason for doing so. Data subjects should be told how personal data they provide may be used. This might be included in application forms or brochures/booklets.

2. processed for specified purposes. Where any planned use of the information falls outside what has been explained to the data subject or what they might expect, consent must be obtained before proceeding.

3. adequate, relevant and not excessive. We must be able to demonstrate that the level of personal information we collect is required for the effective delivery of services.

4. accurate and, where necessary, kept up to date. Where we are making decisions based on such data, we have a responsibility to ensure it is accurate and kept up to date.

5. not kept for longer than is necessary. In principle personal data should not be kept for longer than is necessary for the reason(s) for which it was collected. Some personal data however needs to be retained for legal reasons. Staff must refer to the ELB Record Retention and Disposal Schedule before destroying records.

6. processed in line with the rights of the individual. Data subjects have rights under the Act. These include: right of access to their records, right to have any inaccurate information corrected and a right to prevent processing likely to cause damage or distress.

7. kept secure. Taking appropriate measures to ensure personal data is kept secure is one of the biggest obligations placed on the Board. Data security is equally important for both manual and electronic records and applies throughout all stages of data processing, from obtaining and using to sharing and destruction. A one page fact sheet has been provided on this area.

8. not transferred to countries outside the European Economic Area unless the information is adequately protected. Personal data cannot be transferred to countries which do not have similar personal data legislation to our own.

When dealing with personal data we should always ask ourselves the question; if this was my personal data, how would I like it to be treated?
DATA PROTECTION – PUT SECURITY FIRST

MANUAL RECORDS

- Keep personal data in a locked filing cabinet or drawer.
- Operate a clear desk policy; Lock all personal data away when you are finished with it and at the end of the day.
- Only remove files containing personal information from storage areas when necessary. Their location should be tracked at all times.
- Pupil or client records transferred between Boards should be moved securely. Such files should be hand delivered and signed for or sent by recorded delivery post and marked strictly confidential.
- Destroy personal data by shredding.

ELECTRONIC RECORDS

- Do not store personal data on desktops, laptops or portable media unless protected by encryption software.
- Usernames and passwords provide legitimate users access to Board systems and should not be disclosed to anyone. Always renew passwords when prompted.
- Position monitors so others cannot see personal data. When leaving your desk, lock your PC (by pressing ‘Ctrl, Alt and Del’ keys simultaneously). Log off when leaving for longer periods.
- Never leave personal data at printers. Collect print jobs promptly.
- Emails sent to addresses outside the organisation will be transmitted across the internet. Never send personal data to such addresses.
- Avoid sending personal information by fax. Where this is necessary do it over a secure protocol.
- Never leave laptops/portables/media unattended. When transporting any computer media always ensure it is out of sight, either in a glove compartment or boot of a car.

GENERAL

- Personal information should only be passed on, on a need to know basis.
- Do not allow sensitive conversations to be overheard.
- Guard against people seeking information by deception.
- If working from home treat that environment like your work environment. Do not allow friends/family access to any information.

For further advice please contact the WELB Data Protection Officer or FOI Officer on 02882411247 / 02882411553.