

## SECURITY MEASURES

The Data Protection Act 1998 places obligations on Data Controllers (Schools) to operate good practice for the fair and secure handling of personal data. These obligations are set out in the 8 Data Protection Principles (set out in the Guide).

The 7<sup>th</sup> Principle states:

***'Appropriate technical and organisational measure shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'***

Schools need to take appropriate care of the personal data, taking account of the availability and disclosure of data held in both manual and electronic form.

The security measures should be appropriate to the level of potential harm that could be caused if the personal data were disclosed, lost or damaged without the proper authorisation.

As the Principal (the Data Controller) you will need to consider the following:

- Physical security: what physical security measures are in place to safeguard information. Look at access controls to:
  - School
  - Offices/Classrooms;
  - Filing cabinets;
  - Manual folders;
  - Printed material
  - Computer systems;
  - Floppy disks
- Security measures for computer systems:
  - Passwords;
  - List of authorised users and what they can and can't access;
  - Taking information off-site;
- Training and supervision of staff and contractors.
  - Cover not only awareness of Act and its obligations but also releasing information by phone, in person, in writing.
  - Should include all staff, not just teachers and office personnel.
- Disposal of personal data, e.g. old PCs, printed material, disks, manual files/records.

### **Business Continuity**

You will need to consider the risks carefully and develop contingency plans (business continuity plans) to ensure that in the event of a threat becoming a reality the operation of the school can be recovered swiftly. How will you recover lost personal data?

## **Threats**

Threats can come from many sources ranging from natural disasters to deliberate or accidental incidents.

- Natural sources such as floods and storms;
- Problems such as fire, system and electrical faults;
- Accidents of all kinds;
- Criminal behaviour including break-ins, theft and computer hacking;
- Misuse of systems, e.g. private business in the workplace, carelessness, ignorance of systems and procedures and use of equipment, record handling.

## **Disclosure of Personal Data**

You should identify and examine the routine disclosures of information both internally within the school (all staff); and externally to other people or organisations (e.g. C2K, ELBs, DE, Social Services).

You should also identify any transfers or disclosure of information outside of the EEA (European Economic Area), examining the necessity of such transfers/disclosures and eliminating any that are not required for the operation of the school.

If your school maintains a web site and publishes personal data then this is regarded as a 'Worldwide' transfer (see Notification purpose: Advertising, Marketing.....).

## **Compliance**

In order to demonstrate compliance with the 7<sup>th</sup> Principle it is recommended that the school draw up written evidence of issues identified above. It may be that further action is required (either by the school or jointly with the SEELB), but in the first instance an initial audit should be done to identify controls, training needs and action required.