

Data Protection

The Data Protection Act 1984 has now been replaced by the Data Protection Act 1998, which is based on the European Data Protection Directive. The 1998 Act applies to both manual and computerised personal files and requires transparency in the use of information and emphasises the need for privacy and access by individuals. Information on how to make a request for access to personal data under the Act may be obtained from the Human Resources Officer.

The primary purpose of current data protection legislation is to protect individuals against possible misuse of information about them held by others. It is the policy of the College to ensure that all members of the College and its staff are aware of the requirements of data protection legislation.

There are eight principles put in place by the Data Protection Act 1998 to make sure that individual's information is handled properly. These principles require that personal data shall:

- be fairly and lawfully processed;
- be processed for limited purposes
- be adequate, relevant and not excessive;
- be accurate and kept up-to-date;
- not be kept for longer than is necessary;
- be processed in accordance with data subject's rights;
- be kept secure;
- not be transferred to countries without adequate protection.

Under the terms of the new Act, processing of data includes any activity to do with the data involved. All staff or other individuals who have access to, or who use, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised person. Examples of data include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with the principles outlined above. In order to comply with the first principle (fair and lawful processing), at least one of the following conditions must be met:

- the individual has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- processing is required under a legal obligation;
- processing is necessary to protect the vital interests of the individual;
- processing is necessary to carry out public functions;
- processing is necessary in order to pursue the legitimate interests of the controller or third parties (unless it could prejudice the interests of the individual).

In the case of sensitive personal data which includes information about racial or ethnic origins; political beliefs; religious or other beliefs; trade union membership; health; sex life; criminal allegations, proceedings or convictions, there are additional restrictions and explicit consent will normally be required.

In relation to security (Principle 7), the Data Controller (the College) must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data and sets out specific considerations for ensuring security. Staff and other individuals should be aware that guidelines and regulations relating to the security of manual filing systems and the preservation of secure passwords for access to relevant data held on computer should be strictly observed.

Staff should also note that personal data should not normally be provided to parties external to the College. Special arrangements apply to the exchange of data between the University and the colleges. For further guidance on this, please contact the [Human Resources Officer](#).

Individuals are encouraged to familiarise themselves with the general aspects of Data Protection contained in the College's guidelines to the Act, referred to above and with any specific measurements recommended by the College or their Department relevant to the particular nature of their work. Further information and advice may be obtained from the Human Resources Officer or at: www.informationcommissioner.gov.uk.