WADHAM COLLEGE

DATA PROTECTION POLICY AND CODE OF PRACTICE

The College regards the primary purpose of data protection legislation as being to protect individuals from possible misuse of information about them held by others. The College's policy is to ensure that all members of the College (employees, students and visitors) are fully aware of the requirements of data protection legislation and of their individual responsibilities to this connection.

Code of Practice

The Data Protection Act (1984) involved legislation in relation to automated data records. The Data Protection Art (1998) increased the scope of the legislation, extending its coverage to any "relevant filing system" (including manual records.)

The current legislation covers personal data, whether held on computer or in a "relevant filing system". The College recognises its obligation to abide by the data protection principles embodied in the legislation. These principles require that personal data shall:

- Be processed fairly and lawfully.
- Be held only for specified purposes and not used or disclosed in any way incompatible with those purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up-to-date.
- Not be kept longer than necessary for the particular purpose.
- Be processed in accordance with the data subject's rights.
- Be kept secure.
- Not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection.

In addition, the College is required to nominate a Data Protection Officer. In the College's case this office is fulfilled by the Domestic Bursar.

The legislation provides individuals with rights in connection with personal data held about them. It provides individuals with the right to access data concerning themselves (subject to the rights of third parties.) It also includes the right to seek compensation through the courts for damages and distress suffered by reason of inaccuracy or the unauthorised destruction of wrongful disclosure of data. Access requests should be addressed to the College's Data Protection Officer.

Under the terms of the legislation, 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 such data include address lists and contact details as well ad 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. Further details of the requirements for consent may be found in the relevant legislation and by enquiry of the College's Data Protection Officer or at:www.informationcommissioner.gov.uk.

In relation to security (Principle 7), the College undertakes to ensure 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 ensuing security. College members 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.

College members should also note that special arrangements apply to the provision of data to third parties (which include the University as well as outside bodies.) The College notes that personal data about an individual placed on the World Wide Web is likely to breach the provisions of the legislation (in that information is being transmitted outside the EU) unless the individual whose data is used has given his or her consent. It is important that all those preparing web pages, address lists and the like, are aware of these provisions, and seek advice from the Data Protection Officer if in doubt.

A failure to comply with the provisions of the legislation may render the College or the individuals involved, liable to prosecution as well as giving rise to civil liabilities. 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 measures recommended by the University Department relevant to the particular nature of their work. Further information and advice may be obtained from Data Protection Representatives:

- Fellows' Records – Warden.
- Student Records – Senior Tutor.
- Development Business – Development Director.
- Staff Personnel Records – Domestic Bursar.

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.

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 measures recommended by the College or their University 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.