JESUS COLLEGE POLICY ON DATA PROTECTION

The primary purpose of current data protection legislation is to protect individuals against possible misuse of information about them held by others. Under the provisions of the Data Protection Act 1984, specific legislation was introduced in relation to automated data. The impact of the legislation has now been considerably widened under the terms of the Data Protection Act 1998, which came into force on 1 March 2000. 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 under their individual responsibilities in this connection.

The Act covers personal data, whether held on computer or in a “relevant filing system”. Further guidance and definitions can be found on the University’s website: http://www.admin.ox.ac.uk/councilsec/dp/defs.shtml.

The College is obliged to abide by the data protection principles embodied in the Act. These principles require that personal data shall:

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

The Act 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 relevant transitional relief and 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 or wrongful disclosure of data. Access requests should be addressed to the College Data Protection Officer (the Estates Bursar).

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. Further detail of the requirements for consent may be found in the guidelines referred to above.

In relation to security (principal 7), the Data Controller (the College) must take appropriate technical and organizational 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 special arrangements apply to the provision of data to third parties (which include the University and other colleges as well as outside bodies).

One effect of principal 8, which restricts the transfer of material outside the European Area, is that personal data about an individual placed on the World Wide Web is likely to breach the provisions of the Act unless the individual whose data is used has give his or her explicit 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.

The Act specifies arrangements for the notification of processing undertaken by the Institution. The College has in place wide-ranging registrations under the 1998 Act that can be accessed online at http://www.ico.gov.uk/. The College’s registration number is Z6661163. Any members of staff who are uncertain as to whether their activities or proposed activities are included in the University’s notification should contact the Data Protection Officer in the first instance.

A failure to comply with the provisions of the Act may render the College, or in certain circumstances 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 Oxford University’s guidelines to the Act. Further information and advice may be obtained from the College’s Data Protection Officer (the Estates Bursar).