

UNIVERSITY COLLEGE BIRMINGHAM

DATA PROTECTION POLICY STATEMENT

1. It is our policy to take all necessary steps to ensure that personal data held by the College about its employees, students, customers, suppliers and all other individuals is processed fairly and lawfully. The College will take all reasonable steps to implement this policy.
2. It is the policy of the College to ensure that all relevant statutory requirements are complied with and that internal procedures are monitored periodically to ensure compliance.
3. The College will implement and comply with the eight Data Protection Principles contained in the Data Protection Act 1998 (“the Act”) which promote good conduct in relation to processing personal information. These Principles are:-
 - (i) Personal data shall be processed fairly and lawfully.
 - (ii) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
 - (iii) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
 - (iv) Personal data shall be accurate and, where necessary, kept up to date.
 - (v) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
 - (vi) Personal data shall be processed in accordance with the rights of data subjects under the Act.
 - (vii) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, damage to, personal data.
 - (viii) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. The attention of all staff is drawn to the data protection rules and procedures laid down by the College from time to time. Staff have a duty to follow these rules and procedures and to co-operate with the College to ensure this policy is effective. Disciplinary action may be taken against any member of staff who fails to comply with these rules and procedures.
5. The College has a responsibility to ensure that personal data dealt with in the course of its business is handled in accordance with statutory requirements and reasonable steps will be taken by all concerned to ensure this duty is observed.
6. The College will consult with staff periodically to ascertain what measures should be taken to increase awareness of data protection issues and to ensure that all necessary measures are taken to make this policy effective.
7. The College will take such measures as may be necessary to ensure the proper training, supervision and instruction of all relevant staff in matters pertaining to data protection and to provide any necessary information.
8. The College will monitor on an ongoing basis compliance with the provisions of the Act by third party processors of the College's data.
9. The person having overall responsibility for data protection will be the College Secretary. A team of colleagues will have delegated responsibility for the following areas:-

Staff records	-	Director of Personnel & Student Services
Student records	-	Assistant Principal - Information Services
Supplier/Consultant records	-	Assistant Principal - Finance
Customer records	-	Vice Principal - Academic
10. Each member of staff will have immediate responsibility for data protection matters in his/her own area of work. Any queries should be raised with the relevant officer in 9 above.
11. The Information Technology Development Committee has been charged with periodically reviewing data security arrangements, monitoring the risk of exposure to major threats to data security, reviewing and monitoring security incidents, and establishing and implementing initiatives to enhance data security.

DATA PROTECTION RULES AND PROCEDURES

1. Responsibility

- 1.1 Data protection is a responsibility shared by all staff of the College. Staff must familiarise themselves with and observe at all times these Rules and Procedures relating to data protection, the Data Protection Policy Statement and any additional instructions which may be issued from time to time.
- 1.2 The person having overall responsibility for data protection within the College will be the College Secretary. A team of colleagues will have delegated responsibility for the following areas:-
- | | |
|-----------------------------|--|
| Staff records | - Director of Personnel & Student Services |
| Student records | - Assistant Principal - Information Services |
| Supplier/Consultant records | - Assistant Principal - Finance |
| Customer records | - Vice Principal - Academic |
- 1.3 Each member of staff will have responsibility for data protection matters in his/her own immediate area of work, but in addition, many employees doing their normal duties may be required to process personal data within the meaning of the DPA 1998; for example, information about customers, suppliers or fellow staff members.
- 1.4 Staff who have any questions, comments or suggestions in relation to data protection should contact the relevant officer in 1.2 above.
- 1.5 The Information Technology Development Committee has been charged with periodically reviewing data security arrangements, monitoring the risk of exposure to major threats to data security, reviewing and monitoring security incidents, and establishing and implementing initiatives to enhance data security.

2. Processing Personal Data

- 2.1 Over and above the information for which the College has obtained the individuals consent to hold/process and for which the Data Protection Registrar has confirmed the consent to hold/process, there may be occasions when additional information about an individual needs to be held/processed. In such instances, the College is required to obtain the consent of the individual to hold/process this additional information about him/her. Staff will be advised when such consent is required and how such consent should be obtained. If you are in any doubt about whether consent is required from an individual, you should contact the relevant officer detailed in 1.2. Remember that an 'individual' could

be a student, a colleague, a customer, supplier or other third party with whom you have dealings.

- 2.2 When additional consent is required, the individual concerned will be provided with the following:-
 - The purpose or purposes for which the data is intended to be held/processed;
 - The identity of the party to whom the information may be given.
 - 2.3 Personal data should only be used for the purpose or purposes advised to the individual and not for any ancillary purpose. For example, if an individual such as a supplier or customer was informed that his/her data would only be used for marketing purposes, then such data cannot be used for any purpose other than marketing.
 - 2.4 Personal data held about an individual should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is held. All opinions and/or statements of fact recorded about the individual must be accurate and relevant to the purpose or purposes for which the personal data is held.
 - 2.5 Personal data held about an individual must be kept up-to-date and accurate, and all staff are required to notify the Personnel Unit of changes in their circumstances so that accurate, up-to-date records can be maintained. Students are required to notify their mentor/year manager of any changes.
 - 2.6 If the individual staff member or student, as the case may be, withholds his/her consent or if his/her consent is not provided, then immediate reference should be made to the College Secretary for instruction.
3. **Security of Data**
- 3.1 All personal data held by the College is to be treated as strictly confidential.
 - 3.2 Personal data must not be disclosed to anyone outside the College unless the individual concerned has consented to such disclosure, or the College Secretary has given you a specific instruction to do so.
 - 3.3 Personal data must not be disclosed to any unauthorised employees. The College Secretary will establish and control personal data access.

- 3.4 User passwords will be issued to relevant employees who deal with computerised personal data. Such user passwords are not to be disclosed to any third party or unauthorised employee.
- 3.5 Individuals will have a right, on written request, to obtain a copy of such personal data relating to him/her held by the College as is required under the Data Protection Act 1998. All requests by individuals for information about personal data the College holds about them must be referred, immediately on receipt, to the relevant officer identified in 1.2 of this document who will co-ordinate the response to the relevant individual. The College reserves the right to charge a fee for this service. The College Secretary will determine the level of fee to be charged.
- 3.6 All security breaches, or suspected security breaches, relating to unauthorised access to or disclosure of personal data must be reported immediately to the College Secretary.

Disciplinary action may be taken against any employee who fails to comply with the above rules and procedures.