

DATA PROTECTION POLICY

The purpose of this document is to set out Stroud College's policy towards data protection.

The College needs to keep information about employees, students and others to carry on its business as a further education college. Data includes information held in written records as well as data held on computers. The College must comply with the eight Data Protection Principles which are set out in the Data Protection Act 1998 (the Act). In summary these state that personal data must be:

1. Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Adequate, relevant and not excessive for those purposes;
4. Accurate and kept up to date;
5. Not kept for longer than is necessary for that purpose;
6. Processed in accordance with the data subject's rights;
7. Kept safe from unauthorised access, accidental loss or destruction;
8. Not transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

It is college policy that all staff or others who process or use any personal information must follow these principles at all times and comply with the Act. Breach of the act can lead to both criminal and civil liabilities for the College. Procedures will be established to aid compliance with the Act.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the policies and procedures made by the College from time to time. Any failure to follow these can therefore result in disciplinary proceedings.

Rights of staff, students and others

All staff, students and other users are entitled to:

- Know what data the College holds and processes about them and why;
- Know how to gain access to it whether it is held on computer or in certain paper files. A charge of £10 may be made on each occasion access is requested;
- Know how to keep it up to date;
- Know what the College is doing to comply with its obligations under the Act.

Responsibilities of staff, students and others

Staff have a responsibility to ensure that any personal data which they hold is kept securely and that personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Students who, for whatever reason, process personal data must notify the college Data Protection Officer.

Others who have access to personal data must do so in compliance with the Act and with relevant codes of practice.

A working assumption should be that all written or computer stored data (including comments, notes and references) about any student or member of staff could become disclosed to that person and all such notes should be made with this in mind.

Other matters which will be covered in procedures.

It is the College policy to make as much information public as possible however the college will define what is available to the public for inspection. Anyone who has good reason for wishing details in public documents to remain confidential should contact the Data Protection Controller.

Generally the College can only process personal data with the consent of the individual. To process 'sensitive' data express consent must be obtained. Agreement to the College processing personal data is a condition of acceptance of a student onto any course and a condition of employment for staff. A refusal to give consent to process data will result in the relevant offer being withdrawn.

Policies and procedures will be published on the use of college computer facilities however there should be no expectation of privacy in any stored work or in messages sent or received. When sending e mails on the College's system, the sender is consenting to the processing of any personal data contained in that e mail and is explicitly consenting to the processing of any sensitive personal data contained in that e mail. If individuals do not wish the College to process such data they should communicate it by other means.

The college has the right to monitor any aspect of its telephone and computer systems. To ensure compliance with the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, staff are required to consent to the College doing so. The college will notify staff and students of any other monitoring such as CCTV.

The college will identify a member of the senior management team as the Data Protection Controller and it will identify a specific point of contact for enquiries regarding student data and staff data.

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the outstanding fees have not been paid, or all books and equipment have not been returned to the College.

Specific guidance will be given to staff who may provide references on behalf of present or former staff or students.

The College will define retention periods for different forms of information. Information will not be kept longer than is appropriate.

Detailed procedures will underpin the implementation of this policy

Document history: Approved by the finance & general purposes committee: 26 November 2001 Approved by the corporation: 6 December 2001 Owned by Director of Finance
--