

SOUTH DEVON COLLEGE

Data Protection Policy

1. SCOPE

- 1.1 This policy applies to all staff and students and covers the possession and use of personal information, including electronic images.

2. POLICY STATEMENT/STATEMENT OF INTENT

- 2.1 South Devon College needs to keep certain information about its employees, students and other users of the College's facilities to allow it, for example, to monitor performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised, students recruited as well as to ensure compliance with legal obligations and the requirements of funding bodies. To comply with the law on data protection, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

3. STATUTORY FRAMEWORK

- 3.1 The College will comply with the Data Protection Principles which are set out in the Data Protection Act 1998. In summary these state that personal data shall:
- (a) be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
 - (b) be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
 - (c) be adequate, relevant and not excessive for those purposes
 - (d) be accurate and kept up to date
 - (e) not be kept for longer than is necessary for that purpose
 - (f) be processed in accordance with the data subject's rights
 - (g) be kept safe from unauthorised access, accidental loss or destruction
 - (h) not be transferred to a country outside the European Union, unless that country has equivalent levels of protection for personal data.
- 3.2 Those processing personal information must ensure that these principles are followed at all times.

4. POLICY IMPLEMENTATION

4.1 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 rules and policies made by the College from time to time. Any failure to follow the policy can therefore result in disciplinary action.

In addition, failure to comply with the Data Protection Act 1998 may result in prosecution.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should initially raise the matter with their line manager. If the matter is not resolved it should be raised as a formal grievance.

4.2 Notification of Data Held and Processed

All staff, students and other users are entitled to know:

- (a) what information the College holds and processes about them and why
- (b) how to gain access to it
- (c) how to keep it up to date
- (d) what the College is doing to comply with its obligations under the Data Protection Act 1998.

The College will therefore provide all staff with a standard form of notification, which will state all the types of data the College holds and processes about them, and the reasons for which it is processed. The College will seek to do this at least once every three years. Students will have access to their e-ILP, which details some of the information that is held about them.

4.3 Responsibilities of Staff

- (a) All staff are responsible for:
 - (i) checking that any information that they provide to the College in connection with their employment is accurate and up to date
 - (ii) informing the College of any changes to information which they have provided, for example, change of address
 - (iii) checking the information that the College will send out from time to time, giving details of information kept and processed about staff
 - (iv) informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.
- (b) If and when, as part of their responsibilities, staff collect information about other people, (for example about students course work, opinions about

ability, references, details of personal circumstances), they must comply with the guidelines for staff, which are set out in Appendix 1 to this document.

All staff are responsible for ensuring that:

- (i) any personal data which they hold is kept securely
 - (ii) personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party (exceptions include the police or doctors/hospitals in an emergency)
 - (iii) staff should note that unauthorised disclosure will usually be a disciplinary matter, and may, in some cases be considered gross misconduct. Failure to comply with the Data Protection Act 1998 may result in prosecution.
- (c) Personal information should be:
- (i) kept in a locked filing cabinet or drawer
 - (ii) password protected if it is computerised
 - (iii) kept on portable computer storage devices only if these are kept securely.

4.4 Student Obligations

- (a) Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, mobile phone numbers etc are notified in accordance with the College procedure.
- (b) Students who use the College computer facilities must do so in accordance with the log in script displayed on screen and the IT Policy.

4.5 Rights to Access Information

- (a) Staff, students and other users of the College have, as data subjects, the right to access any personal data that is being kept about them. Any person wishing to exercise this right should complete the College 'Application for Personal Data Release' form and hand it in to the Head of Information, Performance and Funding.
- (b) South Devon College makes a charge of £10 on each occasion that access is requested, although the College has discretion to waive this.
- (c) The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

4.6 Publication of College Information

- (a) Information that is already in the public domain is exempt from the Data Protection Act 1998. It is the College policy to make as much information

public as possible, and in particular the following information will be available for public inspection:

- (i) Names of College Governors and Register of Interest of Governing Body members and senior staff with significant financial responsibilities (for inspection during normal office hours only)
 - (ii) List of key staff
 - (iii) Photographs of key staff and Governors
- (b) The College internal phone list will not be a public document.
- (c) Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Controller.

4.7 Subject Consent

- (a) In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, implicit agreement must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous convictions.
- (b) Some courses or jobs will bring the applicant into contact with children including young people between the ages of 16 and 18. The College has a duty of care under the Children Act and other legislation to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to others.
- (c) The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use this information in the protection of the health and safety of the individual, but will need consent to process, for example, in the event of a medical emergency.
- (d) All prospective staff and students will be asked to sign a 'Consent to Process' form (Learning Agreement in the case of students), regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

4.8 Processing Sensitive Information

- (a) Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure the College is a safe place for everyone, to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this

is available from the Head of Information, Performance and Funding.

4.9 The Data Controller and the Designated Data Controller

- (a) Under the Data Protection Act 1998 the College as a Further Education Corporation is the data controller, and thus the Governing Body is ultimately responsible for implementation. However, there are designated Data Controllers dealing with day to day matters. The first point of contact for enquirers is:

Head of Information, Performance and Funding, Room 3.131,
Telephone 01803 540576.

4.10 Examination Marks

- (a) Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

4.11 Retention of Data

- (a) The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. A copy of the College's Retention Policy can be obtained from the Head of Information, Performance and Funding.

4.12 Disposal of Data

- (a) When personal data is no longer required, or has passed its retention date, paper records will be shredded. If there is a significant amount of material which cannot be dealt with by normal shredding machines, this will be placed in red plastic sacks, available from the Estates Department, and a request made to the Estates Department for collection.
- (b) Computerised records must be permanently deleted, with particular care taken that 'hidden' data cannot be recovered. The IT Helpdesk can advise of permanent deletion of computerised records.

4.13 Conclusion

- (a) Compliance with Data Protection legislation is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution.
- (b) Any questions or concerns about the interpretation or operation of this policy should be taken up with the Head of Information, Performance and Funding.

5. MONITORING OF POLICY

The Policy will be monitored via the College's ILT Committee and the Senior Management Team.

Appendices

- 1 Staff Guidelines for Data Protection
- 2 Application for Personal Data Release
- 3 Application for Personal Data Release to a Third Party
- 4 Standard Form for consent to process sensitive data
- 5 Standard Form for notification of Personal Data held by the College
- 6 Guidelines for archiving

SOUTH DEVON COLLEGE

Data Protection - Staff Guidelines

1. Staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references or as part of a pastoral or academic supervisory role. The College will ensure, through registration procedures (declarations on application/enrolment forms and Learning Agreements), that all students give their consent to this sort of processing and are notified of the categories of processing as required by the Data Protection Act 1998. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:
 - (a) general personal details such as names and addresses
 - (b) details about class attendance, course work marks and grades and associated comments
 - (c) notes of personal supervision, including matters about behaviour and discipline.

Where the functionality and capacity exists, this information should be stored on existing College systems such as EBS and should not be held on ad-hoc spreadsheets or databases.

2. Information about a student's physical or mental health; sexual life, political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should use the College standard form.

Examples: recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of tutorial support.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Data Protection Policy. In particular staff must ensure that records are:
 - (a) accurate
 - (b) up-to-date
 - (c) fair
 - (d) not duplicated on other systems
 - (e) kept and disposed of safely, and in accordance with the College policy.
4. The College will designate staff as 'authorised staff'. These are the only staff authorised to hold or process data that are:
 - (a) not standard data, or

(b) sensitive data.

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary and

- in the best interest of the student, staff member, other user of the College's facilities, or the College, and
- he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

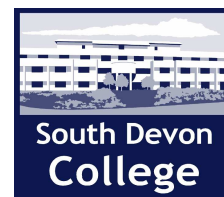
This should only happen in very limited circumstances.

Example: A student is injured and unconscious, but in need of medical attention and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

5. Authorised staff will be responsible for ensuring that all data is kept securely.
6. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with College policy.
7. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with College policy.
8. Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied it is in the best interests of the student or staff member to collect and retain the data?
- Is the information already collected and stored elsewhere by the College?
- Have you reported the fact of the data collection to the authorised person within the required time?



APPLICATION FOR PERSONAL DATA RELEASE

I, _____ (insert name) wish to have access to either
(delete as appropriate)

1. All the data that the College currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that the College has about me in the following categories (please tick):

<input type="checkbox"/>	Academic marks or course work detail
<input type="checkbox"/>	Academic or employment references
<input type="checkbox"/>	Attendance records
<input type="checkbox"/>	CCTV images at _____ (insert location) on _____ (insert date and time)
<input type="checkbox"/>	Disciplinary records
<input type="checkbox"/>	Health and medical records
<input type="checkbox"/>	Personal details including name, address, date of birth etc
<input type="checkbox"/>	Political, or religious details
<input type="checkbox"/>	Statements of opinion about my abilities or performance
<input type="checkbox"/>	Other information: Please list below

Name: _____

Address: _____

I was a student*/member of staff*/or otherwise connected* with the College during the period from _____ (insert date) to _____ inclusive. *Please delete as appropriate.

I understand that a fee of £10 will be payable. Cheques should be made payable to:
South Devon College.

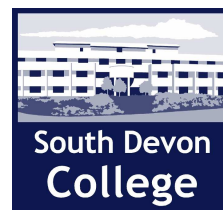
Signed: _____ Date: _____

South Devon College use

Personal data released by:

Date:

A copy of this form should be provided with the evidence



APPLICATION FOR PERSONAL DATA RELEASE TO A THIRD PARTY

I, _____ (insert name)

authorise South Devon College to release personal data to:

Name: _____

Signed: _____ Date: _____

Data Protection

South Devon College adheres to the 8 principles of the Data Protection Act 1998

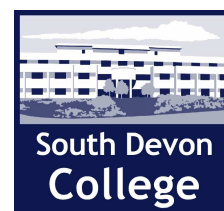
- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Personal data shall be accurate and, when necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 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 of the rights and freedom of data subjects in relation to the processing of personal data.

South Devon College use

Personal data released by:

Date:

A copy of this form should be provided with the evidence



CONSENT TO PROCESS SENSITIVE DATA

I, _____ (insert name) give my

Consent to South Devon College recording and processing information about me in the following categories:

- 1 Race and ethnic origin
- 2 Physical or mental health or medical condition
- 3 Criminal records - a statutory requirement

The information will be used for the following purpose:

	Administering sick pay and sick leave processes
	Managing attendance/absence control
	Checking suitability and fitness to work at the College
	Checking suitability and fitness for a place on a College course
	Administering the College and statutory maternity leave and pay schemes
	Managing and maintaining a safe College environment
	Managing duties and obligations under the Disability Discrimination Act
	Statistical Monitoring to ensure that the College complies with Equal Opportunities good practice

I understand that this information will be used only for the purpose set out in the statement above, and my consent is conditional upon the College complying with its obligations under the Data Protection Act 1998.

This document will be stored in a secure location.

The particular information to be recorded and processed has been shown to me on _____ (insert date) and I confirm that it is correct.

Note: The College Data Protection Policy stipulates that individuals will be advised of any sensitive data to be processed about them.

Signed _____

Date _____

Notification of Personal Data held by the College

This notice is served as part of the requirement of the Data Protection Act 1998. It sets out the types of personal data that South Devon College currently holds about you, and gives details of that data.

When you receive this form you should:

- check that the information included on you is correct
- tell the Human Resources Manager if there are any errors or if any of the data is incomplete
- ask to see any of the information if you want further details.

We cannot provide all of the data on this form, but you do have the right to access most of the information we have about you.

We currently hold information in the following categories:

- 1 **Personal details: this includes, name, address, qualifications, next of kin**
(insert details of this information for the data subject to check)

- 2 **Details of physical and/or mental health: this includes details about specific conditions individuals may suffer from, for example, asthma or diabetes; information about pregnancy, sickness absence and any medical reports received by the College**
(insert details of this information for the data subject to check)

- 3 **Details about work performance, including notes of appraisals etc**
(insert details of this information for the data subject to check)

- 4 **Personnel information including details on start date, pension and pay, current disciplinary or grievance matters, deductions from salary, loans**
(insert details of this information for the data subject to check)

- 5 **Details about any criminal record**
(insert details of this information for the data subject to check)

- 6 **Other categories**
(insert details of this information for the data subject to check)

Signed on behalf of the College

Date

Guidelines for Retention of Records/Archiving

Consideration to be given to extending the appendix from the Financial Regulations to one based on JISC.

Note: This will be undertaken as part of the review of Financial Regulations to be carried out by March 2009.