SOUTH DEVON COLLEGE

Data Protection Policy
RPO1-IT1

Document control

Version	Date	Author(s)	Notes on Revisions
1.0	2008	Lesley Taylor	Original
1.1	June 2008	Dan Hallam	Update following practical use
1.2	November 2013	Dan Hallam	Update following ESF guidance
1.3	April 2016	Dan Hallam	Update following ESF guidance
1.4	March 2017	Dan Hallam	Appendix 2: Updated with link to online shop.
1.5	April 2018	Dan Hallam	To reflect GDPR

1. PURPOSE AND SCOPE

1.1 This policy applies to all staff and students and covers the processing of personal data as defined by Data Protection legislation.

2. DEFINITIONS

2.1 Data refers to any information relation to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This may include name, id number, or location data and applies to automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

2.2 Sensitive personal data are special categories of data and include for example race, ethnicity, religion, trade union membership but excludes criminal convictions or offences but require special safeguards when processing.

2.3 Data or information about the College or information about groups of people from which individuals cannot be identified is covered by the Freedom of Information Policy.

3. DUTIES OF THE COLLEGE

3.1 South Devon College acts as a data processor on behalf of its funding and performance accountability agencies and as a data controller for some of its operational requirements.

3.2 South Devon College processes personal data relating to its staff and learners to effectively manage learning and to meet its statutory obligations as a further education college.

3.3 This processing will be undertaken within the principles of the Data Protection legislation and the College is responsible for, and being able to demonstrate,

compliance with the principles.

3.4 The post of Assistant Principal – Systems, Information, Performance and Apprenticeships is the Data Protection Officer for the College.

4. STATUTORY FRAMEWORK/PRINCIPLES

4 The College will comply with the Data Protection legislation and staff processing personal information must ensure that the principles of the legislation are followed at all times.

4.1 The College processes data under the following legal bases:

4.1.1 Consent
4.1.2 Contract
4.1.3 Legal obligation
4.1.4 Public task
4.1.5 Legitimate interest

4.2 The College processes Special Category Data in line with the lawful bases above and in line with the conditions below:

4.2.1 The data subject has given consent to the processing of those personal data for one or more specified purposes
4.2.2 Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the College or the data subject in the field of employment and social security and social protection law
4.2.3 Processing is carried out in the course of the College's legitimate activities with appropriate safeguards, ensuring that personal data are not disclosed outside of the College without the consent of the data subjects
4.2.4 Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

4.3 The College processes Criminal Offence Data in line with the lawful bases above and in its official capacity

5. POLICY IMPLEMENTATION

5.1 Specific staff responsibilities

5.1.1 Managers in the College will be responsible for the following systems and data groups:

5.1.1.1 Learner Information and Exams Manager – Student data
5.1.1.2 Finance Manager – Finance data
5.1.1.3 Helpzone Manager – Enquiry and funding support data
5.1.1.4 Section Head – SEND and EHCP support data
5.1.1.5 Human Resources Manager – Staff data
5.1.1.6 Marketing, PR & Communications Manager – Public website and marketing data
5.1.1.7 Property Services Manager – CCTV and site access data
5.1.1.8 IT Manager – IT data
5.1.1.9 Quality Manager – learning resource, feedback data
5.1.1.10 Apprenticeship and Employer Engagement Manager - Employer and external stakeholder

5.2 **All staff are responsible for:**

5.2.1 checking that any information that they provide to the College in connection with their employment is accurate and up to date

5.2.2 informing the College of any changes to information which they have provided, for example, change of address

5.2.3 checking the information that the College holds on its HR system(s)

5.2.4 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.

5.3 If and when, as part of their responsibilities, staff process data about other people, (for example about students course work, opinions about ability, references, details of personal circumstances), they must comply with the legislation and can use the guidelines for staff as a starting point, which are set out in Appendix 1 to this document.

5.4 All staff are responsible for ensuring that personal data shall be:

5.4.1 processed lawfully, fairly and in a transparent manner in relation to individuals.

5.4.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

5.4.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5.4.4 accurate and, where necessary, kept up to date - every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5.4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

5.4.6 processed in a manner that ensures appropriate security of the personal data , including protection against unauthorised or unlawful processing and against the accidental loss, destruction or damage.

5.5 Student Obligations

5.6 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 using LEAP or through a member of staff.

5.7 Students who use the College computer facilities must do so in accordance with the acceptable use statement displayed on screen and the relevant contracts and

agreements.

5.8 Individual rights

5.9 Staff, students and other users of the College have, as data subjects, individual rights under Data Protection legislation. The college will administer these rights in the following ways.

5.9.1 **Right to be informed** – this will be achieved at the point of collection with further details published in the privacy statement published on the College website

5.9.2 **Right of access** - data subjects have the right to access their personal data that the College process. Any person wishing to exercise this right should complete and submit the College 'Application for Personal Data Release'.

5.9.3 There is no charge for dealing with a subject access request but where requests are manifestly unfounded or excessive, particularly because they are excessive, a reasonable fee will be charged to take into account the administrative costs or the College will refuse to respond.

5.9.4 Due to the nature of the data we process, we may hold large amounts of information about an individual. Where this is the case we may ask the data subject to specify the information the request relates to or consider the request is manifestly unfounded or excessive.

5.9.5 The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 1 month unless there is good reason for delay in which case this may be extended by a further two months. In such cases, the reason for delay will be explained in writing to the data subject making the request.

5.9.6 **Right to rectification** – The College will update (within 1 month of receipt of the request) factual information when told personal data is incorrect and are satisfied that the information should be amended. Requests can be submitted verbally or in writing. Matters of opinion may not be amended and we will write to the data subject with reasons of where we will not amend the data despite their request.

5.9.7 **Right to erasure** – The College will consider requests for erasure carefully and any requests should be submitted to the Assistant Principal. Where the basis for processing public duty or legal obligation, the College will refuse the request with a written explanation to the data subject. Where elements of the data record may be deleted without prejudice to the basis for processing, the College will comply with the request.

5.9.8 **Right to restrict processing** – where a data amendment request or right to erasure request is being processed, the College will consider a request to restrict processing. If the restriction prevents the College carrying out its public duty or legal obligations the request will be refused with written explanation provided to the data subject.

5.9.9 **Right to data portability** – where the College processes data based on consent or contract and processing is carried out by automated means, individuals have the right to request data in a structured, commonly used and machine readable form.

5.9.10 **Right to object** – where the College is processing personal data based on legitimate interests or in the performance of its public interest, for direct marketing or for statistical purposes, the data subject has the right to object to processing. With the exception of direct marketing where there is no exemptions or grounds to refuse, the College will assess whether the grounds for processing override the interest, right and freedoms of the data subject and will inform the data subject of the decision

5.9.11 **Rights relating to automated decision making including profiling** – the College does not process any personal data in this way.

5.10 Publication of College Information

5.11 Personal information that is already in the public domain is exempt from the Data Protection Act 1998. The following information will be available to the public:

5.11.1 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)

5.11.2 List of key staff

5.11.3 Photographs of key staff and Governors

5.12 The College internal phone and other such lists will not be a public document.

5.13 Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Assistant Principal.

5.14 Personal information may be released where requested under the Freedom of Information Act and is considered appropriate for release.

5.15 Sharing personal information

5.16 The College will maintain and make public privacy notices documenting how it processes data including who it makes it available to. The processing of data by the College will be based on the principle of safeguarding staff and students and responsibilities to perform the College's educational duties.

5.17 Where subject access requests are made by a third party, these will be considered under the data protection legislation and this policy and where appropriate and reasonable, consent will be sought from the data subject before data is shared.

5.18 Data subjects should be aware that under the lawful processing bases above and the data protection legislation, consent may have already been provided through regular processing, or data may be released for legal purposes.

5.19 In most circumstances, information can be shared with other agencies without individual's consent where there is a safeguarding concern. The statutory guidance from the DfE on 'Keeping children safe in education' states that "Fears about sharing information **cannot** be allowed to stand in the way of the need to promote the welfare and protect the safety of children."

5.20 Retention of Data

5.21 The College will keep some forms of information for longer than others. This will be determined by the type of data, the purpose for which is was processed, requirements of College funding agencies, and for historical and statistical processing.

5.22 To comply with European Social Fund requirements, project and student information relating to the submission of records through the Individualised Learner Record file, predominantly paper enrolment forms and EBS records will be retained according to the published ESF guidance.

5.23 Specifically, enrolment information and all ESF documentation during the period of 2000 to 2006 will be retained until at least 1/2/2021; and enrolment information relating to the period 2007 to 2013 will be retained until at least the end of 31 December 2022 or unless otherwise advised by the ESF Managing Authority; and enrolment information relating to the period 2014 to 2020 will be retained until at least the end of 31 December 2030 or unless otherwise advised by the ESF Managing Authority.

5.24 Disposal of Data

5.25 When personal data is no longer required, or has passed its retention date, it will be disposed of in accordance with data protection legislation.

5.26 Data protection by design and default

5.27 A data protection impact assessment (DPIA) must be carried out to identify and minimise the data protection risks of a project. This may include documenting the reasons for not carrying a full DPIA.

5.28 The IT Security Policy should be considered alongside the DPIA to ensure that appropriate technical and organisational measures are robust.

5.29 Personal data breaches

5.30 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

5.31 All breaches should be reported to the Assistant Principal - Systems, Information, Performance and Apprenticeships promptly by following the College procedure. This will establish the likelihood and severity of the resulting risk to people's rights and

freedoms. Failure of staff to report a breach may result in disciplinary action.

5.32 Where there is a risk identified, the Assistant Principal - Systems, Information, Performance and Apprenticeships will notify the ICO without delay but not later than 72 hours after becoming aware of it.

5.33 Where the breach results in a high risk to the rights and freedoms of individuals, the College will inform those concerned directly and without undue delay.

5.34 Appointing contractors who access the college's personal data

5.35 Where the college appoints a contractor who is a processor of the college's personal data, sufficient due diligence checks and contracts are required before processing. Due diligence includes ensuring the contractor meets their requirements of data protection legislation.

5.36 Any contract and evidence of due diligence must be in writing.

5.37 Complaints

5.38 Complaints about the policy or the handling of personal information should be raised through the College Complaints Procedure in the first instance. Complainants can then contact the Information Commissioner if the complaint is not resolved to their satisfaction.

5.39 Conclusion

5.40 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 criminal prosecution.

5.41 Any questions or concerns about the interpretation or operation of this policy should be taken up with the Assistant Principal – Systems, Information, Performance and Apprenticeships.

6. RELATED POLICIES AND FURTHER GUIDANCE

6.1 Freedom of Information
6.2 IT Security & Internet Usage Policy (including Data Loss Policy)
6.3 Contract of Employment
6.4 Code of Conduct
6.5 Safeguarding Policy
6.6 CCTV (& Body Worn Camera) Policy

7. STATEMENT OF THE COLLEGE'S APPROACH TO THE ENVIRONMENT AND TO SUSTAINABILITY

7.1 The College affirms its commitment to integrate sustainable and eco-friendly policies and practices into all its activities by operating in a manner that promotes energy and materials conservation and waste reduction. We also commit to encouraging others with whom we do business to analyse, reduce

and manage their own environmental impacts and risks where possible.

8. PREVENT DUTY STATEMENT

8.1 South Devon College and South Devon High School are fully committed to safeguarding and promoting the welfare of all learners. We recognise that safeguarding against radicalisation and extremism is no different from safeguarding against any other vulnerability. All our staff, learners and services are expected to uphold and promote the fundamental principles of British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.

This statement reinforces our expectation that staff are fully engaged in being vigilant about radicalisation and extremism; that they overcome any professional disbelief that such issues will happen here and ensure that they work alongside each other, professional bodies and external agencies to ensure that our learners are safe from harm.

9. MONITORING OF POLICY

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

Actions	Date
Signed off – [HR]	22/06/18
Signed off – [Clerk to Governors]	19/07/18
Signed off – [SMT/ Principalship]	19/07/18
Approved – [Resources Committee]	19/07/18
Next Review due	February 2019

10. APPENDICES

10.1 Staff Guidelines for Data Protection
10.2 Application for Personal Data Release
10.3 Application for Personal Data Release to a Third Party
10.4 Police Request for Disclosure of Personal Data
10.5 Personal Data Breach Procedure

SOUTH DEVON COLLEGE

Appendix 1: Staff Guidelines for Data Protection

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 pemission to this sort of processing and are notified of the categories of processing as required by the Data Protection legislation. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

   1.1. general personal details such as names and addresses
   1.2. details about class attendance, course work marks and grades and associated comments
   1.3. notes of personal supervision, including matters about behaviour and discipline.
   1.4. 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 discuss their needs with the Assistant Principal - Systems, Information, Performance and Apprenticeships.

   2.1. 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:
   3.1. accurate
   3.2. up-to-date
   3.3. fair
   3.4. not duplicated on other systems
   3.5. kept and disposed of safely, and in accordance with the College policy.

4. 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.

5. Before processing any personal data, all staff should consider the checklist.

6. Staff Checklist for Recording Data

   6.1. Do you really need to record the information?
   6.2. Is the information 'standard' or is it 'special category'?
   6.3. If it is special category, have you discussed this with the Assistant Principal - Systems, Information, Performance and Apprenticeships?
   6.4. Has the student been told that this type of data will be processed?
   6.5. Are you authorised to collect/store/process the data?
   6.6. If yes, have you checked with the data subject that the data is accurate?
   6.7. Are you sure that the data is secure?
   6.8. 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?
   6.9. Is the information already collected and stored elsewhere by the College?
   6.10. Have you reported the fact of the data collection to the authorised person within the required time?

Appendix 2: 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):

	Academic marks or course work detail
	Academic or employment references
	Attendance records
	CCTV images at (insert location) on (insert date and time)
	Disciplinary records
	Health and medical records
	Personal details including name, address, date of birth etc
	Political, or religious details
	Statements of opinion about my abilities or performance
	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.

Signed:_____Date: _____

South Devon College use	
Personal data released by:	Date:

A copy of this form should be provided with the evidence

Appendix 3: APPLICATION FOR PERSONAL DATA RELEASE TO A THIRD PARTY

I,_____(insert name)

authorise South Devon College to release personal data to:

_____

Name: _____

Signed:_____Date: _____

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

South Devon College use	
Personal data released by:	Date:

A copy of this form should be provided with the evidence

Appendix 4: Police Request for Disclosure of Personal Data
Under Section 28(1) or 29(3) of the Data Protection Act 1998

From:

Name ……

Address ……

……

……

Contact numbers ……

To:

Name Learner Information Services Office, South Devon College
Address Vantage Point, Long Road, Paignton, Devon TQ4 7EJ

1. Please provide the following information:

   Name and address ☐ Attendance information ☐ Other ☐

2. Information requested:

3. I certify that the data is required for national security purposes or prevention or detection of crime or for the apprehension or prosecution of offenders and that failure to disclose the data would likely to prejudice these matters.

4. The requested data are required for case reference …… It is possible that this data may have relevance in future to as yet unidentified offences and it may need to be used in such an event. It will not be used in any way incompatible with the purpose for which it is being disclosed.

5. I understand that if any data on this form is omitted or wrong I may be committing an offence under data protection legislation.

6. Signed…… Date……
   Name & number…….. Rank: PC

Appendix 5: Personal Data Breach Procedure

This section outlines the procedure that should be followed when any member of College staff becomes aware of a data breach.

The procedure comprises a checklist, a risk assessment and a high level workflow. Completion of the checklist should be overseen by the incident owner in consultation as appropriate with curriculum Assistant Principal, and the Assistant Principal Systems, Information, Performance and Apprenticeships.

This procedure should be used by any staff that loses data and are otherwise involved in managing an incident. Appropriate documentation of the decisions taken and the reasons for them should be maintained, even where the breach is not reported to the ICO or individuals notified.

Step 1 – A member of staff who becomes aware of a personal data breach should complete the checklist below and send to the curriculum Assistant Principal, and the Assistant Principal Systems, Information, Performance and Apprenticeships.

Step 2 – The curriculum Assistant Principal, and the Assistant Principal Systems, Information, Performance and Apprenticeships will assess the severity of the incident including the risk to people's rights and freedoms, the nature and scale of the breach, and the personal data affected.

This will include an assessment of the negative consequences of the breach: If not addressed in an appropriate and timely manner, it may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality or personal data protected by professional secrecy or any other significant economic or social disadvantage to the person concerned.

Step 3 – The Assistant Principal Systems, Information, Performance and Apprenticeships will notify Principalship of the incident and recommend whether there is a risk to people's rights and freedoms and whether it should be reported to the ICO.

Step 4 – The Assistant Principal Systems, Information, Performance and Apprenticeships will recommend whether there is a high risk to the rights and freedoms of individuals and whether they should be notified.

Step 5 – Where a decision to report the breach to the ICO is taken, the Assistant Principal Systems, Information, Performance and Apprenticeships will do this in accordance with the ICO guidance.

Step 6 – Where a decision to notify the individuals is taken, the Assistant Principal Systems, Information, Performance and Apprenticeships will coordinate this describing:

- The nature of the breach
- The name and contact details of the data protection officer where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.