SOUTH DEVON COLLEGE

DATA PROTECTION POLICY

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
1.6	July 2021	Kelly Sooben	Scheduled review
1.7	August 2022	Kelly Sooben	Annual review
1.8	August 2023	Kelly Sooben	Annual review

1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors, parents and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The College has implemented this Data Protection Policy to ensure all College Employees are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

College Employees will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any of the College employee's contract of employment and the College reserves the right to change this

Policy at any time. All members of College staff are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. ABOUT THIS POLICY

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

3.1. **College** – South Devon College

3.2. **College Employees** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary Employees hired to work on behalf of the College.

3.3. **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

3.4. **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

3.5. **Data Protection Officer –** Our Data Protection Officer is Kelly Sooben, Vice Principal People & Resources and can be contacted at kellysooben@southdevon.ac.uk

3.6. **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

3.7. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

3.8. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

3.9. **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.
Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

3.10. **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

3.11. **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

3.12. **Data Processing -** is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

4. South Devon College makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the College the College will ensure that the third party takes such measures in order to maintain the College's commitment to protecting data. In line with current data protection legislation, understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

5. DATA PROTECTION PRINCIPLES

5.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

5.1.1. processed lawfully, fairly and in a transparent manner;

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

5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

5.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and

5.1.6. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2. These principles are considered in more detail in the remainder of this Policy.

5.3. In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

6. DATA PROTECTION PROCEDURES

The College has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:
· it appoints or employs employees with specific responsibilities for:
a. the processing and controlling of data
b. the comprehensive reviewing and auditing of its data protection systems and procedures
c. overviewing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

· it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
· it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
· it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
· it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Organisation

- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Organisation understands that consent must be freely given, specific, informed and unambiguous. The Organisation will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time

· it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences

· it is aware of the implications of international transfer of personal data

6. PERSONAL DATA

6.1. Data Protection Laws require that the College personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

6.2. The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

6.3. If College employees feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College employees have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

7. LAWFUL USE OF PERSONAL DATA

7.1. In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing]

7.2. In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

7.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If College employees therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

8. TRANSPARENT PROCESSING – PRIVACY NOTICES

8.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has adopted the following privacy notices: Employee Privacy Notice and Student Privacy Notice.

8.2. If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

8.3. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College employees therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the College employee's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

9. DATA SECURITY

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

In addition, employees must:

· ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them

· ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people

· refrain from sending emails containing sensitive work related information to their personal email address

· check regularly on the accuracy of data being entered into computers

10. DATA BREACH

10.1. Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and College employees must comply with the College's Data Breach Notification Policy. Please see paragraphs 10.2 and 10.3 for examples of what can be a Personal Data

breach. Please familiarise yourself with it as it contains important obligations which College employees need to comply with in the event of Personal Data breaches.

10.2. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

10.3. There are three main types of Personal Data breach which are as follows:

10.3.1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College employee is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

10.3.2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, employee Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

10.3.3. **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

11.4 The Governing Body of the College will receive an annual report from the College's Data Protection Officer (DPO) regarding data breaches that have been reported to the ICO in the past year. Data breaches that are reported to the ICO and result in specific action/fines will be immediately reported to the Chair of the Governing Body and then formally reported at the next full Governing Body meeting.

11. ACCESS TO DATA

- Relevant individuals have a right to be informed whether the College processes personal data relating to them and to access the data that the Organisation holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- · a form on which to make a subject access request is available from the Data Protection Officer. The request should be made to the Data Protection Officer.
- · the College will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the College will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.
- Relevant individuals must inform the College immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The College will take immediate steps to rectify the information.
- For further information on making a subject access request, employees should refer to our subject access request policy.

12. COLLEGE EMPLOYEES'S GENERAL OBLIGATIONS

12.1. All College employees must comply with this policy.

12.2. College employees must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

12.3. College employees must not release or disclose any Personal Data:

12.3.1. outside the College; or

12.3.2. inside the college - to College employees not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

12.4. College employees must take all steps to ensure there is no unauthorised access to Personal Data whether by other College employees who are not authorised to see such Personal Data or by people outside the College.

13. MARKETING AND CONSENT

13.1. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any

marketing, Data Protection Laws require that this is only done in a legally compliant manner.

15.TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Organisation are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the College of any potential lapses and breaches of the College's policies and procedures.

16. RECORDS

The Organisation keeps records of its processing activities including the purpose for the processing and retention periods in its Records & Retention policy. These records will be kept up to date so that they reflect current processing activities.

17. AUTOMATED DECISION MAKING AND PROFILING

a. Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

Automated Decision Making happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

b. Any Automated Decision Making or Profiling which the College carries out is only done once the College is confident that it is complying with Data Protection Laws. If College Employees therefore wish to carry out

any Automated Decision Making or Profiling College Employees must inform the Data Protection Officer.

c. College Employees must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

d. The College does not carry out Automated Decision Making or Profiling in relation to its employees.

18. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

a. The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be undertaken prior to the processing via a Data Protection Impact Assessment (**"DPIA"**). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

   i. describe the collection and use of Personal Data;

   ii. assess its necessity and its proportionality in relation to the purposes;

   iii. assess the risks to the rights and freedoms of individuals; and

   iv. the measures to address the risks.

b. A DPIA is completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

c. Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

d. Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College considers whether it needs to carry out a DPIA as part of the project initiation process. The College will carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

e. Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

i. large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

ii. large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

iii. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

f. All DPIAs must be reviewed and approved by the Data Protection Officer.

19. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

a. Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

b. So that the College can ensure it is compliant with Data Protection Laws College Employees must not export Personal Data unless it has been approved by the Data Protection Officer.

c. College Employees must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.