

SOUTH DEVON COLLEGE
STUDENT PRIVACY NOTICE

Document control

Version	Date	Author(s)	Notes on Revisions
1.0	April 2018	Dan Hallam	New Policy for GDPR
2.0	July 2021	Kelly Sooben	Policy review
3.0	July 2022	Kelly Sooben	Annual review

Owner	SLT Lead	Author	Frequency of review	Next review date	Approval Committee	Next approval Committee Date	Date of last EIA
KS	LF	KS	Annually	July 2023	SLT		

We are the data controller and processor of personal information about you. We are: South Devon College. Our address is: Vantage Point, Long Road, Paignton, Devon, TQ4 7EJ.

Our Data Protection Officer is Vice Principal People & Resources. If you have any questions about this policy or the ways in which we use your personal information, please contact our Data Protection Officer via email at enquiries@southdevon.ac.uk.

This privacy notice has been prepared in accordance with the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act 2018.

What does 'personal data' mean?

Your personal data is any information that identifies you directly or indirectly. Examples of personal data are your name, address, identification number etc. Some information about you is called 'special category data'. This includes race, ethnic origin, political opinions, religious beliefs, trade union membership, genetic and biometrical information, health, sex life and sexual orientation. This type information receives additional protection.

What does 'student' mean?

A student is a child, young person or adult who is cared for or enrolled at the College.

What does 'processing' mean?

'Processing data' 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

Does the College have the right to process my personal data?

One of the seven major data processing principles is to ensure that personal data is processed lawfully, fairly, and transparently.

To comply with this principle, Chapter 6 of the GDPR requires any organization processing personal data to have a valid legal basis for that personal data processing activity. These are:

Consent

The individual has given clear consent for the College to process their personal data for a specific purpose.

Performance of a Contract

The processing is necessary for a contract the College has with an individual have with the individual

Legitimate Interest

The processing is necessary for the College's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Vital Interest

The processing is necessary to protect someone's life.

Legal Requirement

The processing activity is necessary for a legal obligation.

Public Interest

A processing activity that would occur by a government entity or an organization acting on behalf of a government entity.

What categories of personal information are received from third parties?

The College collects and processes information from third parties about students and applicants.

This information may be about the person's:

- academic history
- health and wellbeing
- safeguarding
- support plans
- domestic and financial circumstances
- interactions with other agencies including the police

The College may get such information from

- a present of previous school, College, university, or employer
- Youth Offending Team • Probation Service
- Local Authorities from across the UK
- Careers South West (CSW)
- Health Professionals
- Student Loan Company
- UCAS
- parents, carers, and guardians

With which organisations and people does the College share personal information?

We may share your personal information with third parties who provide services to the College:

- Local authorities and their partners – this includes Torbay Council, Devon County Council, and Plymouth City Council. Some local authorities contract out their

services, for example to Careers South West and information will be shared with them.

- Contracted services – this includes Stagecoach and PayMyStudent to help us administer your travel and bursary information, The University & College Admissions Service (UCAS) (for students who apply for or study an HE course with us), The Student Loans Company (for students who apply for or take a student loan), The UK Visa & Immigration Service, Auditors, Ofsted or other formal regulatory bodies for the education sector, and third parties who are contracted to provide IT services to us.
- Awarding organisations – this includes City & Guilds, OCR, Pearson, Ascentis, University of Plymouth. We share the information so they can formally accredit your learning and achievements.
- Local authorities and their partners – this includes Torbay Council, Devon County Council, Careers South West
- Funding agencies – this includes the Education and Skills Funding Agency, Office for Students, Student Loans Company, and the Department for Education. This allows us, and in turn our funding agencies, to claim funding for the education we provide.
- NHS and other health services – this includes GPs, CAMHs
- The police and other enforcement agencies – there may be legal and legitimate reasons we share information with these agencies to protect you or others
- Health and wellbeing charities – this includes The Children’s Society Checkpoint
- Local press – this includes the Herald Express where we would like to share your success with them for publication.
- National and regional education awards – this includes the Association of College where we would like to share your success with them to help us win awards and receive recognition from external bodies.

For how long does the College keep personal information?

The College typically keeps personal data for 6 years + the current academic year. 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.

What rights do data subjects have over their personal data?

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.

To exercise these rights, you or your authorised representative can contact the DPO via the college website, email, telephone, or letter.

The College processes your data to:

- Provide education to you
- Monitor and report your educational progress
- Provide appropriate pastoral care
- Assess the quality of our work
- Comply with the law regarding education and safeguarding
- Support you to progress onto further studies or employment

We have a range of technical and operational measures in place to protect personal data from accidental destruction, misuse or disclosure.

Data stored electronically is governed by role-based access control, based on the minimum required by for an employee to carry out their duties. Data is encrypted in transit, and all systems require secure passwords for access. All personal data is secured behind firewalls to prevent unauthorised access, with implicit deny rulesets in place. Comprehensive anti-virus, web filtering and email filtering tools are in place, along with strict patching cycles to minimise cyber-attacks and potential security exploits.

All employees attend data protection awareness training as part of induction to the College. Employees are only given access to personal data if they need to use it as part of their role and access to information is strictly controlled. Only staff with the relevant training have access and access is removed when staff leave the College.

We have a suite of policies, procedures and codes of practice to enable us to appropriately manage our obligations under data protection.

How we transfer your personal information outside Europe.

We do not store or transfer your personal data outside Europe.

Changes to our privacy policy

- We keep our privacy policy under regular review. Any changes we make to our privacy policy in the future will be notified to you by email.