Data Protection Policy

plus other relevant information

Southport College

KING GEORGE V COLLEGE

Data Protection Policy

1.Data Protection Policy

1.1 The College

Southport College takes its responsibilities with regards to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) very seriously. Southport College (the College) is the legal entity for both Southport and KGV colleges and this policy applies to all data held by the College. This document provides the framework for effective management of Data Protection and helps to ensure compliance when processing personal data.
The College is the data controller and holds personal data about students, parents, staff and other individuals in order to carry out its business and provide its services eg name, address, date of birth, etc.

The College will comply with the Data Protection Act 2018 by ensuring that Personal Data is:

- **Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.**
- **Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.**
- **Adequate, relevant and not excessive for those purposes.**
- **Accurate and kept up to date.**
- **Not be kept for longer than is necessary for that purpose.**
- **Processed in accordance with the data subject's rights.**
- **Protected against unauthorised or unlawful processing and against accidental loss or destruction or damage.**
- **Not transferred to a country outside the european economic area, unless that country has equivalent levels of protection.**

1.2 Information

The college needs to keep certain information about its employees, students and suppliers 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 and legal obligations to funding bodies and government complied with.

1.3 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. Any failures to follow the policy can therefore result in disciplinary proceedings. Any member of staff, or any student, who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the appropriate designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

1.4 Notification of Data Held & Processed

All staff, students and other users are entitled to:

- **Know what information the college holds and processes about them and why.**
- **Know how to gain access to it.**
- **Know how to keep it up to date.**
- **Know how to have it erased**
- **Know what the college is doing to comply with its obligations under the current DPA legislation.**

1.5 Responsibilities of Staff/Students

All staff/students are responsible for:

- **Checking that any information that they provide to the college in connection with their employment/enrolment is accurate and up to date.**
- **Informing the college of any changes to the information provided, i.e. change of address.**
- **Checking the information that the college will send out from time to time, giving details of information kept and processed.**
- **Informing the college of any errors or changes. The college cannot be held responsible for any errors unless the student or member of staff has informed the college of them.**

If, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references or details of personal circumstances), they must comply with the guidelines for staff (see Section 2).

1.6 Data Security

All staff are responsible for ensuring that:

- **Any personal data, which they hold, is kept securely.**
- **Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised party.**

Personal information should be:

- **Kept in a locked filing cabinet: or**
- **In a locked draw: or**
- **If it is computerised, password protected: or**
- **Kept only on encrypted portable media, which is itself kept securely.**
- **Disposed of safely and securely.**
- **If transferred electronically either internally or externally, password protected.**

1.7 Rights of Access to Information

Staff, students and other users of the college have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should put their request in writing addressed to the Data Protection Officer. The college aims to comply with the requests for access to personal information as quickly as possible, but will ensure that it is provided within 1 calendar month.

1.8 Subject Consent

Express consent must be obtained for the processing of sensitive personal data. The college may ask for information about criminal convictions or particular medical conditions. The college will only use this information to ensure the safety of its entire staff and students or in the event of a medical emergency.

Some information does not require consent. This includes:

- **Names and declared conflict of interests of college governors**
- **List of key staff**
- **Photographs of key staff and governors**

Any person who has good reason for wanting details in these lists or categories to remain confidential should contact the Data Protection Officer.

1.9 The Data Controller and the Data Protection Officer

Southport College as a corporate body is the Data Controller under the Act, and the board of governors is therefore ultimately responsible for implementation. The College has an appointed Data Protection Officer to provide advice and guidance, monitor compliance and act as the first point of contact for the ICO and individuals.

1.10 Examination Marks

Students will be entitled to information about their marks for both course work and examinations. However, this may take longer than other information to provide.

1.11 Data Retention

The college will keep some forms of information for longer than others. In general, information about students will be kept for approximately seven years after they leave the college.

This will include:

- **Name and address: academic achievements: copies of any reference written: other personal details as collected at enrolment.**
- **The college will need to keep information about staff for longer periods of time. In general, all information will be kept for 7 years after a member of staff leaves the college. Some information however will be kept for much longer. This will include necessary information such as pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.**
- **The period of time that records will be kept for is specified in the College Data Retention Schedule. It is recognised however, that the College holds records on various electronic data systems and records held here may have different retention periods than those detailed in the schedule.**
  Where this is the case, the College will ensure that the data is held with appropriate technical and organisational security and will be deleted when required.

1.12 Policy Compliance

Compliance with the DPA 2018 is the responsibility of all members of the college. Any 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. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

2. Guidelines for Staff

2.1 Definitions:

2.1.1 Data

Any information which will be or which is being used or processed by a computerised system, or which is recorded with the intention that it will be processed in this way will be "data" for the purpose of the Act. In addition, any information kept as part of a "relevant filing system" will be data. This may include personnel records, or student registers or files which are stored alphabetically as well as information collected with the intention that it will be filed in such a system. It can also include post it notes (if it shows 'intent'). Data can be written information, photographs, or information such as fingerprints or voice recordings, diaries, USB drives, memory sticks and other storage devices.

2.1.2 Personal Data

Information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data, which the college currently has or may have in the future.

For example, application forms marked only with a number will not identify an individual, but put together with the list of numbers and names, will do so.

Personal data will include names and addresses, features such as hair and eye colour which will often be in the form of photographs, ethnic origin, qualifications and experience, details about sick leave and holidays taken, birthdays or marital status.

Any opinion about intentions regarding a person that are recorded, will also be personal data.

2.1.3 Processing

The term "processing" covers almost anything which is done with or to the data, including:

- **Obtaining the data**
- **Recording, or entering data onto the files**
- **Holding data, or keeping it on file, without doing anything to it or with it**
- **Organising, altering or adapting data in any way**
- **Retrieving, consulting or otherwise using data**
- **Disclosing data either by giving it out, by sending it on e-mail, or simply by making it available**
- **Combining data with other information**
- **Erasing or destroying data**

2.1.4 Data Subject

This is an individual about whom personal data is kept.

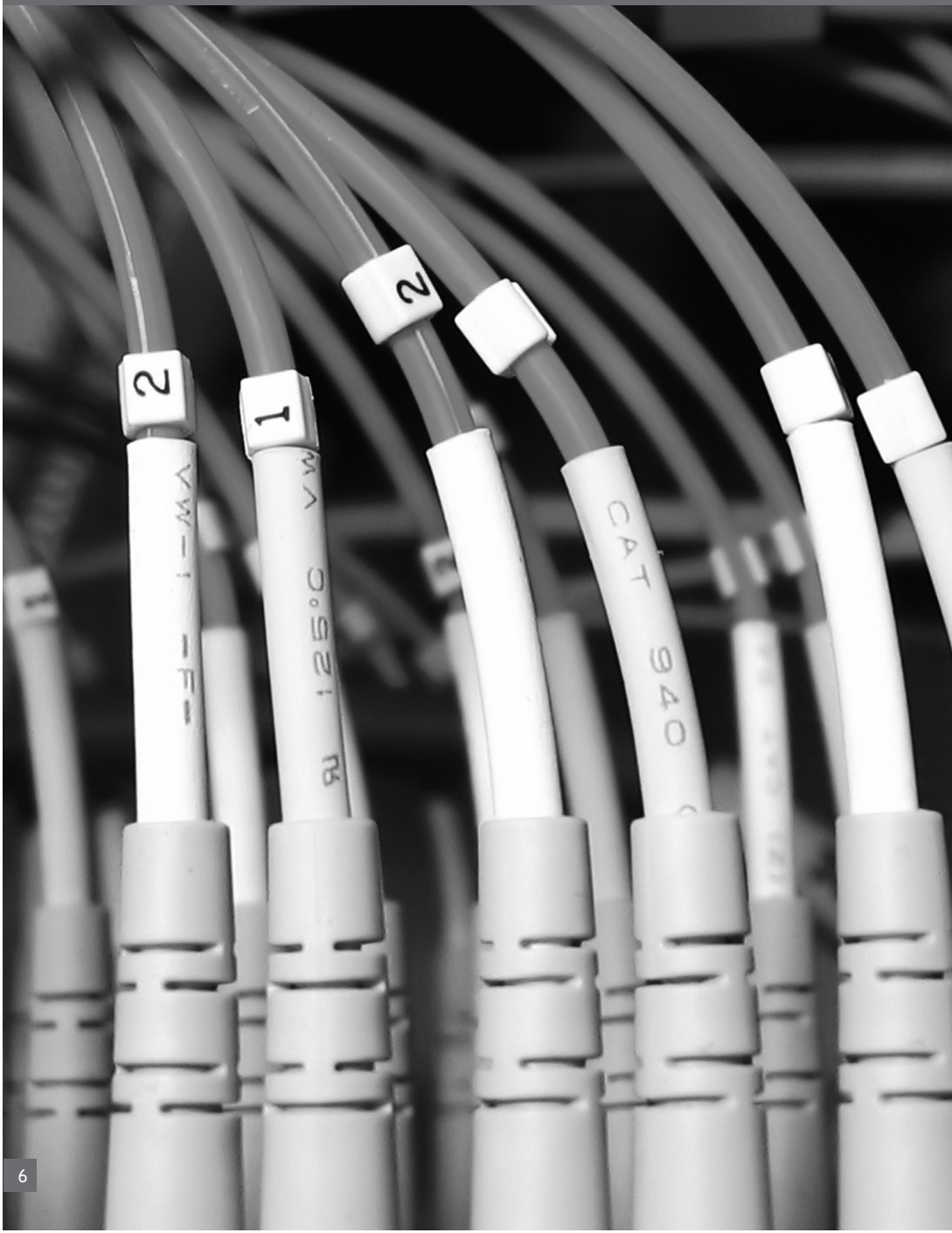
2.1.5 Data Controller

The "Data Controller" is responsible for ensuring that data is collected, stored and processed fairly, for deciding which types of information will be processed and the reason for the processing. The legal responsibility for this will rest with the corporation as a corporate body.

2.1.6 Data Processor

This is either a person or an organisation other than someone employed by the college who processes data for or on behalf of the data controller.

Data Protection Policy



2.1.7 Sensitive Data

Data is considered sensitive if it is about:

- **An individual's race**
- **Political opinions**
- **Religious beliefs**
- **Trade union membership or non-membership**
- **Their physical or mental health**
- **Sex life or sexual orientation**
- **Criminal record**

2.1.8 Consent to Process

One of the requirements of fair processing is that the data subject must agree to the processing. Consent requires that there is some active agreement between the two parties.

2.1.9 Relevant Filing System

The Act extends data protection to paper or manual files if the information contained in them forms part of a "relevant filing system". This is a set of information about individuals, which is structured either by name or by another criterion, such as a course title, so that specific information is "readily accessible" to the person using or processing it.

2.2 Processing of Personal Data

2.2.1

All staff will process data about students on a regular basis; when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The college will ensure through enrolment procedures, that all students give their consent for this sort of processing and are notified of the categories of processing, as required by the Act. The information that staff deal with on a day-to-day basis will be standard and will cover categories such as:

- **General personal details such as name and address**
- **Details about class attendance, course work marks and grades and associated comments**
- **Notes of personal supervision, including matters about behaviour and discipline.**

2.2.2

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 seek advice from the appropriate designated Data Controller.

2.2.3

Before processing any personal data, all staff should consider the following:

- **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?**

2.2.4

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:

- **Accurate**
- **Up-to-date**
- **Fair**
- **Kept securely and disposed of safely**

For further information contact the Data Protection Officer.

2.3 Requests for disclosure of personal data

2.3.1

A disclosure must only take place when any of the following conditions apply:

- **When the permission of the Data Subject is given**
- **Within the college, for authorised functions or registered purposes of the college**
- **Where the disclosure is by order of a Court or compliant with the criteria set out in 2.6.**

2.3.2

Disclosing personal data on the telephone:

Staff must not disclose information over the telephone before the caller's identity has been verified (e.g. by phoning them back on a known number, or by confirming a known reference number, or by discussing some reference details known only to the college and the caller).

2.3.3

If common sense suggests that a particular disclosure should be an exception to the rule (e.g. where someone might be at risk), staff must consult their line manager (as soon as practicable) and make a proper record of the disclosure, to whom it was made and of the circumstances that made the disclosure necessary.

2.3.4

Where disclosure of sensitive information takes place, a note of the disclosure must be recorded on the appropriate files or case papers.

2.3.5

Staff must note that the confidential nature of any personal information supplied must be stressed at all times: so they must not take short cuts and always follow the correct procedure. If in doubt, do not disclose.

2.4 Refusing to disclose Personal Data

2.4.1

Where disclosure of data is refused, staff must explain that they are not allowed to disclose personal data unless the caller's credentials to receive the data have first been verified. Staff must always explain that the reason why they are refusing to give information is one of confidentiality and because the caller has not provided adequate identification. The following is suggested as the basis for a standard explanation: "The Data Protection Act 2018 regulates the use of personal data. It is the College's policy to respect the confidentiality of the personal data in its possession, and because you have not been able to identify yourself properly, I cannot help you. However, if you can call again, and provide satisfactory identification, I may be able to comply with your request".

2.6 Disclosure of Personal Data to Prosecuting Agencies

2.6.1

Section 28 of the Data Protection Act allows for personal data to be disclosed to certain agencies (e.g. Police, Inland Revenue, Customs and Excise, Public Health Authority, etc) for the purpose of:

- **The prevention or detection of crime**
- **The apprehension or prosecution of offenders**
- **The assessment or collection of any tax or duty**

A disclosure of this kind may be made without fear of making an unauthorised disclosure as long as Data Users can prove that they 'had reasonable grounds for believing that failure to make the disclosure in question would have been likely to prejudice any of those matters above'.

2.6.2

If staff receive a request for personal data from a police officer, customs official, Department of Social Security and other official bodies, they must ask for the request to be put in writing on official paper, showing the agency crest.

2.7 Emergencies

2.7.1

There may be circumstances where staff have to disclose personal data in emergencies. If an emergency involves a threat to a Data Subject's health or to prevent injury to a Data Subject, then the disclosure can take place.

2.7.2

A proper record of the disclosure must be made, either at the time, or as soon as possible after the disclosure has occurred. In other urgent situations, staff will have to use their judgement; but in all cases they must keep a formal record of their decision to disclose, and send a note of the disclosure to their line manager.

2.8 'Subject Access' to Personal Data

2.8.1

Staff may be consulted by an individual who wishes to apply formally for Subject Access (i.e. an individual shall be entitled to access any personal data held by a Data User). In these cases he/she must be referred to the Dasta Protection Officer.

2.8.2

All staff must be aware that Subject Access is a separate and formal procedure by which personal data are disclosed to the Data Subject.

Data Protection Policy

2.9 Personal Data on Home Computers/Laptops

2.9.1

The sixth Data Protection Principle states that;

'Appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)'.

The college has no control over the security of home computers and laptops or indeed persons accessing them. There is always the possibility of the home being burgled and the computer being stolen, or, if the files are stored on external drive, CD, DVD or USB drive that these are stolen or lost in transit. The same would apply to paper records (e.g. registers). Anyone who needs to take personal information off site is responsible for ensuring that:

- **Any personal data, which they hold, is kept securely.**
- **Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised party.**

Personal information should be:

- **Kept in a locked filing cabinet: or**
- **In a locked draw: or**
- **If it is computerised, is password protected: or**
- **Kept only on encrypted portable media, which is itself kept securely.**
- **Disposed of safely and securely.**

You should be aware that if you do not follow procedures and the Act is contravened you personally would be responsible and subject to disciplinary action and may be found to be committing an offence and you could be fined.

2.10 Professional Opinions

2.10.1

The Data Protection Act covers any expression of opinion about individuals. For example, teachers may routinely record professional opinions. Opinions may be recorded informally in reports, letters, memos etc in a way that is covered by the Act.

2.10.2

When an opinion is recorded it is good practice to do the following:

- **Make it clear that it is an opinion. The record should show who gave the opinion and when.**
- **If possible provide contact details.**
- **Structure the record so that if someone objects to its accuracy, his or her view or challenge can be included in such a way that it is given proper weight.**

2.10.3

Ensure that when an opinion is disclosed it is not presented as fact.

2.10.4

Examples of good and bad practice:

Example	Good practice	Bad practice
A student gets a copy of a report written by her tutor and disputes an opinion recorded in it. She also provides convincing evidence that it includes incorrect factual information.	The college explains that it has to be kept as a true record of the tutor's professional opinion but agrees to include the student's comments clearly on her file. The correct factual information is recorded but a record of the error may continue to be held to explain possible unforeseen consequences.	The college refuses to record the student's objections to the opinion and only notes the factual inaccuracies.

Head of Information Services

If you have any queries on this leaflet and what it means to you, contact:

Data Protection Officer
Southport College,
Mornington Road,
Southport PR9 8HZ

tel: 01704 500601

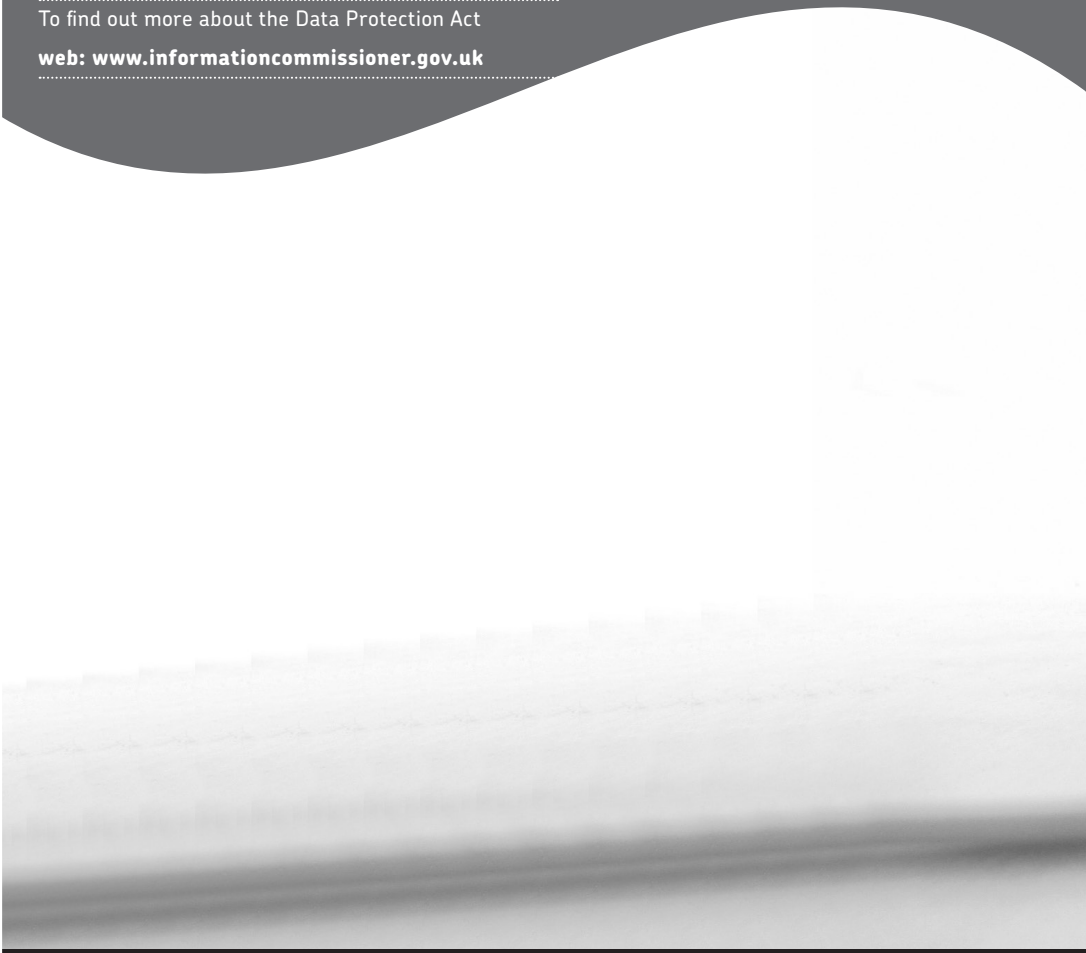
Southport College ICO Registration No: Z6671705

To find out more about the Data Protection Act

web: www.informationcommissioner.gov.uk

Southport College

KING GEORGE V COLLEGE



11546:25/2/21