# Data Protection Policy

| | | | |
|---|---|---|---|
| **Author:** | **Name** | Paris Bonwick | |
| | **Job Title** | Assistant Principal MIS & Apprenticeships | |
| **Date policy reviewed:** | | **Date policy to be reviewed** | |
| **GDPR Impact assessed by:** | P Bonwick | **Date impact assessed:** | |
| **Impact assessed by:** | P Bonwick | **Date impact assessed:** | |
| **Policy approved by:** | | **Date approved:** | |

# Contents

# 1. INTRODUCTION

Southport College reputation and future growth are, in part, dependent on the way that it manages and protects Personal Data. Protecting the confidentiality, integrity and availability of Personal Data is a key responsibility of everyone within the College.

Southport College 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 essential.

The College has implemented this Data Protection Policy so that all College staff know what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and provide a thriving working and learning environment for all.

College staff have access to this policy, along with other related policies on the College's website. A copy of the policy and training on its implementation form part of the staff induction, and all staff will receive information following any significant revisions to the policy . Whilst, this policy is not part of the staff contract of employment and the College reserves the right to change the policy at any time and all members of staff obliged to comply with it at all times.

If you have any queries concerning this policy, please contact our Data Protection Officer, 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) ensures the College complies with its obligations under data protection legislation, including UK GDPR. Personal data must be handled in line with the requirements of all data protection laws that protect the fundamental rights and freedoms of individuals.

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

# 3. DEFINITIONS

3.1. **College** – Southport College (This includes Southport College & King George V Sixth Form College)

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

3.3. **Controller** – Any entity (e.g. company, organisation or person) that determines the purposes and means of collecting and processing personal data.

3.4. **Data Protection Laws** – The UK GDPR (United Kingdom General Data Protection Regulation and all applicable laws relating to the collection and use of Personal Data and privacy and any relevant codes of practice issued by a regulator included in the UK, the Data Protection Act 2018.

3.5. **Data Protection Officer-** The Data Protection Officer (DPO) monitors internal compliance, informs, and advises on the college's data protection obligations and acts as a contact point for data subjects and the Information Commissioner's Office (ICO). They can be contact by emailing: dataprotection@southport.ac.uk

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

3.7. **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.

3.8. **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. 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.

3.9. **Processor** – Any entity (e.g., company, organisation, or person) responsible for processing personal data on behalf 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.

3.10. **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.

## 4. COLLEGE STAFF'S GENERAL OBLIGATIONS

4.1. All College staff must comply with this policy.

4.2. College staff 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.

4.3. College Staff must not release or disclose any Personal Data:

4.3.1. outside the College; or

4.3.2. inside the College, to College Staff not authorised to access the Personal Data,

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

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

## 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 must demonstrate that it complies with them through documented evidence. The College has several policies and procedures in place, including this policy and the documentation referred to ensure that it can demonstrate its compliance.

## 6. LAWFUL USE OF PERSONAL DATA

6.1. To collect and/or use Personal Data lawfully, the College needs to show that its use meets one of several legal grounds. These are:

6.1.1 Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

6.1.2 Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

6.1.3 Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

6.1.4 Vital interests: the processing is necessary to protect someone’s life.

6.1.5 Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

6.1.6 Legitimate interests: the processing is necessary for your 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

6.2. Please click here for more detailed information about the lawful basis for processing data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

6.3. When the College collects and/or uses Special Categories of Personal Data, the College must show that one of several additional conditions is met. These are the following:

6.3.1 Explicit consent

6.3.2 Employment, social security and social protection (if authorised by law)

6.3.3 Vital interests

6.3.4 Not-for-profit bodies

6.3.5 Made public by the data subject

6.3.6 Legal claims or judicial acts

6.3.7 Reasons of substantial public interest (with a basis in law)

6.3.8 Health or social care (with a basis in law)

6.3.9 Public health (with a basis in law)

6.3.10 Archiving, research and statistics (with a basis in law)

6.4. Please click here to see the additional information about special category data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

6.5. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. 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 staff, therefore, intend to change how they use Personal Data, they must notify the Data Protection Officer, who will decide whether their intended use requires amendments to be made and any other controls that need to apply.

## 7. TRANSPARENT PROCESSING – PRIVACY NOTICES

7.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses Personal Data in the form of a privacy notice made available on the College website.

7.2. If the College receives Personal Data about an Individual from other sources, the College can provide the Individual with a privacy notice about how the College will use their Personal Data upon request.

7.3. If the College changes how it uses Personal Data, the College may notify Individuals about the change. If College Staff intends to change how they use Personal Data, please notify the Data Protection Officer who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls that need to applied.

## 8. DATA QUALITY- ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

8.1. Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 7 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

8.2. All College Staff that collect and record Personal Data must ensure that the Personal Data is recorded accurately and is kept up to date. College Staff should ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to that which is necessary for the purpose for which it is collected and used.

8.3. All College Staff that obtain Personal Data from sources outside the College must take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date, and limited to that which is adequate, relevant and limited to data necessary in relation to the purpose for which it is collected and used.

8.4. To maintain the quality of Personal Data, all College Staff that access Personal Data must ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g., for legal reasons or relevant to an investigation).

8.5. The College recognises the importance of ensuring that Personal Data is amended, rectified, erased, or its use restricted where this is appropriate under Data Protection Laws. Any request from an Individual for the amendment, rectification, erasure, or restriction of the use of their Personal Data should be dealt with in accordance with those college processes and procedures relating to Individual rights.

## 9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

9.1. Data Protection Laws require that the College not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

9.2. 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 are contained in the Colleges Retention Policy.

9.3. If College Staff consider 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 Schedule, for example because there is a requirement of law, or if College Staff have any questions about the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

## 10. DATA SECURITY

10.1. The College takes information security very seriously. 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. The College is Cyber Essentials Certified and complies with the rules & regulations of safe keeping of data.

## 11. DATA BREACH

11.1. The College takes information security very seriously; however, it is possible that a security breach could happen, resulting in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens, it is a 'Personal Data breach' and College Staff must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach.

11.2. 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. Most Personal Data breaches happen as a result of action taken by a third party; data breaches can also result from actions taken by College Staff.

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

11.3.1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data, e.g. hacking, accessing internal systems that College Staff are 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 incorrect student, or disclosing information over the phone to the incorrect person;

11.3.2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data, e.g., loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransomware, 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

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

## 12. APPOINTING CONTRACTORS/SUPPLIERS WHO ACCESS THE COLLEGE'S PERSONAL DATA

12.1. If the College appoints a contractor or third party that will act as the College's Processor, then Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

12.2. One requirement of the UK GDPR is that a Controller must only use Processors who meet the requirements of the UK GDPR and protect the rights of Individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they meet their contractual requirements to Data Protection.

12.3. Any contract where an organisation appoints a Processor must be in writing.

12.4. You are considered as having appointed a Processor where you engage someone to perform a service for you, and as part of it, they may gain access to your Personal

Data. Where you appoint a Processor, you, as Controller, remain responsible for the Personal Data.

12.5. The UK GDPR requires the contract with a Processor to contain the following obligations as a minimum:

12.5.1. to only act on the written instructions of the Controller;

12.5.2. to not export Personal Data without the Controller's instruction;

12.5.3. to ensure staff are subject to confidentiality obligations;

12.5.4. to take appropriate security measures;

12.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

12.5.6. to keep the Personal Data secure and assist the Controller to do so;

12.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

12.5.8. to assist with subject access/Individuals rights;

12.5.9. to delete/return all Personal Data as requested at the end of the contract;

12.5.10. to submit to audits and provide information about the processing; and

12.5.11. to tell the Controller if any instruction is in breach of the UK GDPR or other data protection law.

12.6. In addition, the contract should set out:

12.6.1. The subject-matter and duration of the processing;

12.6.2. the nature and purpose of the processing;

12.6.3. the type of Personal Data and categories of Individuals; and

12.6.4. the obligations and rights of the Controller.

## 13. INDIVIDUALS' RIGHTS

13.1. The UK GDPR gives Individuals more control over how their data is collected and stored and what is done with it.

13.2. The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows individuals to exercise their rights.

13.3. The different types of rights of Individuals are reflected in this paragraph.

**13.4. Subject Access Requests**

13.4.1. Individuals have the right under the UK GDPR to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right, but additional information has to be provided,

and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). Also, you will no longer be able to charge a fee for complying with the request.

13.4.2. Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

**13.5. Right of Erasure (Right to be Forgotten)**

13.5.1. This is a limited right for Individuals to request the erasure of Personal Data concerning them where:

13.5.1.1. the use of Personal Data is no longer necessary;

13.5.1.2. their consent is withdrawn, and there is no other legal ground for the processing;

13.5.1.3. the Individual objects to the processing, and there are no overriding legitimate grounds for the processing;

13.5.1.4. the Personal Data has been unlawfully processed; and

13.5.1.5. the Personal Data has to be erased for compliance with a legal obligation.

13.5.2. In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the Individual has a right to object to the processing at any time. Where the Individual objects, the Personal Data must not be processed for such purposes.

**13.6. Right of Data Portability**

13.6.1. An individual has the right to request that data concerning them is provided to them in a structured, commonly used, and machine-readable format where:

13.6.1.1. the processing is based on consent or a contract; and

13.6.1.2. the processing is carried out by automated means

13.6.2. This right is not the same as subject access and is intended to give Individuals a subset of their data.

**13.7. The Right of Rectification and Restriction**

13.7.1. Finally, Individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

## 14. MARKETING AND CONSENT

14.1. 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.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. UK GDPR brought about several significant changes for organisations that market to individuals, including:

14.2.1. providing more detail in their privacy notices, including, for example, whether profiling takes place; and

14.2.2. rules on obtaining consent are stricter and require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

14.3. The College conforms with the Privacy and Electronic Communications Regulations (PECR) that sits alongside data protection legislation. PECR applies to direct marketing, i.e., a communication directed to particular Individuals and covers any advertising/marketing material. It applies to electronic communication, i.e., calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

14.4. Consent is central to electronic marketing; it is essential to liaise with the Data Protection Officer for best practice recommendations to marketing.

14.5. The College has the right to market using a "soft opt-in" if the following conditions were met:

14.5.1. contact details have been obtained in the course of a sale (or negotiations for sale);

14.5.2. the College is marketing its own similar services; and

14.5.3. the College gives the Individual a simple opportunity to refuse to opt-out of the marketing, both when first collecting the details and in every message after that.

## 15. AUTOMATED DECISION MAKING AND PROFILING

15.1. 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.

15.2. Any Automated Decision Making or Profiling that the College carries out can only be done once the College is confident that it complies with Data Protection Laws. Therefore, if College Staff wishes to carry out any Automated Decision Making or Profiling, College Staff must inform the Data Protection Officer.

15.3. Staff must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

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

## 16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

16.1. GDPR laws introduced 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 done before 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. However, it is an assessment of issues

affecting Personal Data that need to be considered before a new product/service/process is rolled out. The process is designed to:

16.1.1. describe the collection and use of Personal Data;

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

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

16.1.4. the measures to address the risks.

16.2. A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals.

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

16.4. Where the College is launching or proposing to adopt a new process, product, or service that involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to 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 that may otherwise occur.

16.5. 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):

16.5.1. 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;

16.5.2. 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

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

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

## 17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

17.1. On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27 June 2025.

17.2. Following the UK's exit from the EU and following the end of the transition period (31st January 2021), restricted transfers from the UK to other countries, including to the EEA, are now subject to transfer rules under the UK regime. These UK transfer rules broadly mirror the EU GDPR rules, but the UK has the independence to keep the framework under review

17.3. Data Protection Laws impose strict controls on Personal Data transferred outside the EEA. A transfer includes sending Personal Data outside the EEA and includes storage of Personal Data or access to it outside the EEA. Giving access to Personal Data to staff outside the EAA 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.

17.4. So that the College can ensure it is compliant with Data Protection Laws, College Staff must not export Personal Data unless the Data Protection Officer has approved the transfer.

## 18. ACCOUNTABILITY

18.1. UK GDPR integrates accountability as a principle, which requires that the College puts in place appropriate technical and organisational measures and be able to demonstrate what it did and its effectiveness when requested.

18.2. The College must demonstrate that it is compliant with the law. Such measures include adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures are aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; that the Data Protection Officer be involved at the planning stage.

18.3. **Staff Accountability.**

All staff shall be responsible for:

18.3.1. Fully complying with the data protection principles, rights and requirements in their handling of personal data.

18.3.2. Performing a Privacy Impact Assessment where new processing of personal data is planned.

18.3.3. Promptly raising concerns about Data Protection or Data Security with the Data Protection Officer.

18.4. Ensuring that all data that they provide to the College in connection with their employment is accurate and up to date and that changes are either made direct onto HR self-service, where relevant, or are notified to Human Resources

18.5. Checking the information that the College holds annually and correcting any errors.

18.6. Any personal details of other people collected by a member of staff such as coursework marks or grades, references to employers or other academic institutions, or any matters about personal circumstances must be collected and stored in accordance with the Data Protection Policy and relevant college guidelines.

# Data Breach Policy

| | | | |
|---|---|---|---|
| **Author:** | **Name** | Paris Bonwick | |
| | **Job Title** | Assistant Principal MIS & Apprenticeships | |
| **Date policy reviewed:** | | **Date policy to be reviewed** | |
| **GDPR Impact assessed by:** | P Bonwick | **Date impact assessed:** | |
| **Impact assessed by:** | P Bonwick | **Date impact assessed:** | |
| **Policy approved by:** | | **Date approved:** | |

**TABLE OF CONTENTS**



## 1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. As an organisation that collects and uses Personal Data, the College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise. The College's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected. The College has therefore implemented this Policy to ensure all College Personnel are aware of what a Personal Data reach is and how they should deal with it if it arises.

College Personnel 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 College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

## 2. ABOUT THIS POLICY

This Policy explains how the College complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the ICO and the affected individuals. The College has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the College deals with and records Personal Data breaches.

**Note: Please refer to the accompanying template Data Breach Notification and Internal Data Breach Register.**

## 3. SCOPE

This Policy applies to all College Personnel who collect and/or use Personal Data relating to individuals.

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

## 4. DEFINITIONS

4.1. **College** – Southport College.

4.2. **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

4.3. **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.

4.4. **Data Protection Officer** – The Data Protection Officer is Lisa Farnhill, and can be contacted at: dataprotection@southport.ac.uk.

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

4.6. **Personal Data** – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

4.7. **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.

## 5. WHAT IS A PERSONAL DATA BREACH

5.1. 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.

5.2. 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.

5.3. A Personal Data breach could include any of the following:

5.3.1. loss or theft of Personal Data or equipment that stores Personal Data;

5.3.2. loss or theft of Personal Data or equipment that stores the College's Personal Data from a College supplier;

5.3.3. inappropriate access controls meaning unauthorised College Personnel can access Personal Data;

5.3.4. any other unauthorised use of or access to Personal Data;

5.3.5. deleting Personal Data in error;

5.3.6. human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);

5.3.7. hacking attack;

5.3.8. infection by ransom ware or any other intrusion on our systems/network;

5.3.9. 'blagging' offences where information is obtained by deceiving the organisation who holds it; or

5.3.10. destruction or damage to the integrity or accuracy of Personal Data.

5.4. A Personal Data breach can also include:

5.4.1. equipment or system failure that causes Personal Data to be temporarily unavailable;

5.4.2. unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;

5.4.3. inability to restore access to Personal Data, either on a temporary or permanent basis; or

5.4.4. loss of a decryption key where Personal Data has been encrypted because this means the College cannot restore access to the Personal Data.

## 6. REPORTING A PERSONAL DATA BREACH

6.1. College Personnel must immediately notify any Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not College Personnel think a breach has occurred or is likely to occur. This allows the College to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the College.

6.2. If College Personnel discover a Personal Data breach outside working hours, College Personnel must notify it to the College's Data Protection Officer as soon as possible.

6.3. College Personnel may be notified by a third party (e.g. a supplier that processes Personal Data on the College's behalf) that they have had a breach that affects College Personal Data. College Personnel must notify this breach to the College's Data Protection Officer and the College's Data Breach Notification Procedure shall apply to the breach.

## 7. MANAGING A PERSONAL DATA BREACH

7.1. There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

7.1.1. Containment and recovery

7.1.2. Assessment of on-going risk

7.1.3. Notification

7.1.4. Evaluation and response

7.2. At all stages of this Policy, the Data Protection Officer and managers will consider whether to seek external legal advice.

## 8. CONTAINMENT AND RECOVERY

8.1. An initial assessment of the Personal Data breach will be carried out by the Data Protection Officer.

8.2. If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected then it will be added to the College's Data Breach Register and no further action will be taken.

8.3. If the Personal Data breach may impact on the rights and freedoms of the individuals affected then the College will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the College's Data Breach Notification Procedure. This will include consideration of:

8.3.1. whether there are any other people within the College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

8.3.2. what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

8.3.3. whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Officer.

8.4. All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

8.5. The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

## 9. ASSESSMENT OF ONGOING RISK

As part of the College's response to a Personal Data breach, once the breach has been contained the College will consider the on-going risks to the College and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the College's Data Breach Notification Procedure.

## 10. NOTIFICATION

10.1. Under Data Protection Laws, the College *may* have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

10.2. Any notification will be made by the Data Protection Officer following the College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

10.3. Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within **72 hours of** when the College becomes aware of the breach unless it is *unlikely to result in a risk to the rights and freedoms of individuals*. It is therefore imperative that College Personnel notify all Personal Data breaches to the College in accordance with the Data Breach Notification Procedure immediately.

10.4. Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is *likely to result in a high risk to the rights and freedoms of individuals.*

10.5. Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

10.6. Where the Personal Data breach relates to a temporary loss of availability of the College's systems, the College does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The College does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

10.7. In the case of complex breaches, the College may need to carry out in-depth investigations. In these circumstances, the College will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

10.8. Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

10.9. When the College notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in

accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the College has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

10.10. The College may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

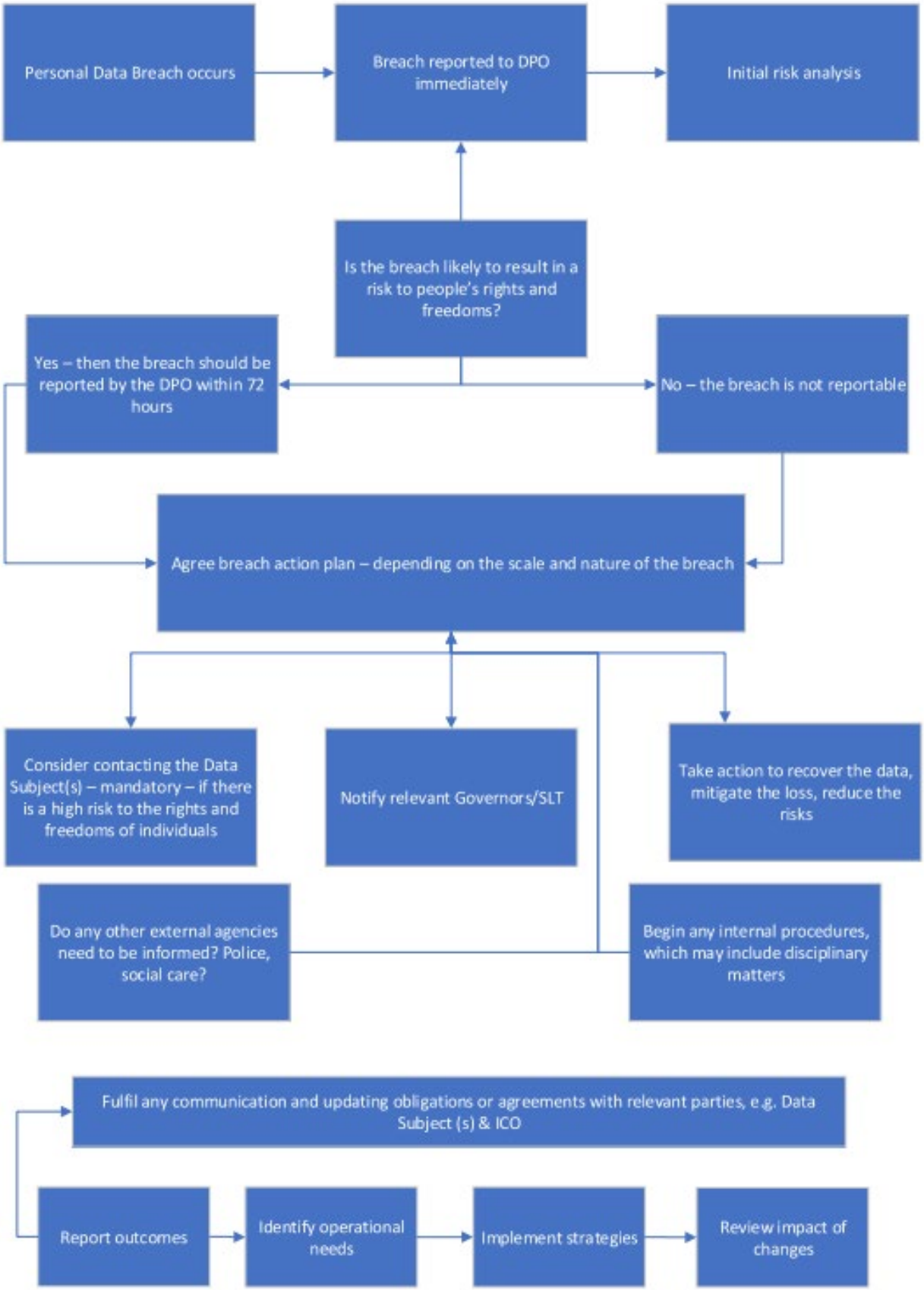
## 11. EVALUATION AND RESPONSE

11.1. It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the College's response to it and the remedial action taken.

11.2. There will be an evaluation after any breach of the causes of the breach and the effectiveness of the College's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

11.3. Any remedial action such as changes to the College's systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

**Annex 1 Data Breach Flow chart**



# RIGHTS OF INDIVIDUALS POLICY

| | | | |
|---|---|---|---|
| **Author:** | **Name** | Paris Bonwick | |
| | **Job Title** | Assistant Principal MIS & Apprenticeships | |
| **Date policy reviewed:** | | **Date policy to be reviewed** | |
| **GDPR Impact assessed by:** | P Bonwick | **Date impact assessed:** | |
| **Impact assessed by:** | P Bonwick | **Date impact assessed:** | |
| **Policy approved by:** | | **Date approved:** | |

# 1. INTRODUCTION

1.1 The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. All individuals have rights over their Personal Data and the College recognises the importance of having an effective Policy in place to allow individuals to exercise those rights in a way that is clear and easy for them. The College has therefore implemented this Rights of Individuals Policy to ensure all College Personnel are aware of what rights individuals have over their Personal Data and how the College makes sure those rights can be exercised.

1.2 College staff are provided with access to this Policy when they start and may receive notifications of any periodic revisions of this Policy. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College staff are obliged to comply with this Policy at all times.

1.3 This Policy applies to all College Personnel who collect and/or use Personal Data relating to individuals.

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

# 2. Definitions

2.1 **College** – Southport College

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

2.3 **Data Protection Laws** – The UK General Data Protection Regulation (UK GDPR) 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.

2.4 **Data Protection Officer** – Our Data Protection Officer can be contacted by email: dataprotection@southport.ac.uk

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

2.6 **Personal Data** – Any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier

2.7 **Processing** – Any collection, use of storage of Personal Data whether on the College's information security systems or in paper form.

2.8 **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.

## 3. College Staff Obligations

3.1 This Policy sets out the rights that individuals have over their Personal Data under Data Protection Laws. If any College staff member receives a request from an individual to exercise any of the rights set out in this Policy, that staff member must:

3.1.1 inform the Data Protection Officer as soon as possible and, in any event, within 24 hours of receiving the request;

3.1.2 tell the Data Protection Officer what the request consists of, who has sent the request and provide the Data Protection Officer with a copy of the request;

3.1.3 not make any attempt to deal with, or respond to, the request without authorisation from the Data Protection Officer.

## 4. What Rights do Individuals have over Their Personal Data?

**4.1 Right of Access Request (RoAR)/ Subject Access Request (SAR)**

4.1.1 Individuals have the right to ask the College to confirm the Personal Data about them that the College is holding, and to have copies of that Personal Data along with the following information:

- the purposes that the College has their Personal Data for;
- the categories of Personal Data about them that the College has;
- the recipients or categories of recipients that their Personal Data has been or will be disclosed to;
- how long the College will keep their Personal Data;
- that they have the right to request that the College corrects any inaccuracies in their Personal Data or deletes their Personal Data (in certain circumstances, please see below for further information); or restrict the uses the College is making of their Personal Data (in certain circumstances, please see below for further information); or to object to the uses the College is making of their Personal Data (in certain circumstances, please see below for further information);
- that they have the right to complain to the ICO if they are unhappy about how the College has dealt with this request or in general about the way the College is handling their Personal Data;
- where the Personal Data was not collected from them, where the College got it from; and
- the existence of automated decision-making, including profiling (if applicable).

4.1.2 The College is not entitled to charge individuals for complying with this request. However, if the individual would like a further copy of the information requested, the College can charge a reasonable fee based on its administrative costs of making the further copy.

4.1.3 There are no formality requirements to making a Right of Access Request (RoAR) and it does not have to refer to data protection law, or use the words Right of Access Request, RoAR, Subject Access Request or SAR. The College will monitor its incoming communications, including post, email, its website and social media pages to ensure that the College can recognise a SAR when it receives it.

4.1.4 The College is required to respond to a SAR/RoAR within one calendar month from the date the College receives it. If the request is complex or there are multiple requests at once, the College

may extend this period by two further months provided that the College tells the individual who has made the request about the delay and the College's reasons for the delay within the first month.

4.1.5 The Data Protection Officer will reach a decision as to the complexity of the SAR/RoAR and whether the College is entitled to extend the deadline for responding.

4.2 **Right to Rectification**

4.2.1 Individuals have the right to ask the College to correct any Personal Data about them that the College is holding that is incorrect. The College is then obliged to correct that Personal Data within one month (or two months if the request is complex).

4.2.2 Where the individual tells the College their Personal Data is incomplete, the College is obliged to complete it if the individual asks the College to do so. This may mean adding a supplementary statement to their personal file for example.

4.2.3 If the College has disclosed the individual's inaccurate Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties of the correction where the College can.

4.2.4 When an individual asks the College to correct their Personal Data, the College is required to do so and to confirm this in writing to the individual within one month of them making the request.

4.3 **Right to Erasure (right to be forgotten)**

4.3.1 Individuals have the right to ask the College to delete the Personal Data the College has about them in certain circumstances but this right is limited in scope and does not apply to every individual. The right to be forgotten applies when:

- the Personal Data is no longer necessary for the purpose the College collected it for;
- the individual withdraws consent and the College has no other legal basis to use their Personal Data;
- the individual objects to the College's processing and there is no overriding legitimate interest for continuing the processing;
- the Personal Data was unlawfully processed; and/or
- the Personal Data has to be erased to comply with a legal obligation.

4.3.2 If the College has disclosed the individual's deleted Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties to delete the Personal Data where the College can

4.3.3 When an individual asks the College to delete their Personal Data, the College is required to do so and to inform the individual in writing within one month of them making the request that this has been done.

**4.4 Right to Restrict Processing**

4.4.1 Individuals have the right to "block" or "suppress" the College's processing of their Personal Data when:

- they contest the accuracy of the Personal Data, for a period enabling the College to verify the accuracy of the Personal Data;

- the processing is unlawful and the individual opposes the deletion of the Personal Data and requests restriction instead;

- the College no longer needs the Personal Data for the purposes the College collected it for, but the College is required by the individual to keep the Personal Data for the establishment, exercise or defence of legal claims;

- the individual has objected to the College's legitimate interests, for a period enabling the College to verify whether its legitimate interests override their interests.

4.4.2 If the College has disclosed the individual's restricted Personal Data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties about the restriction where the College can.

4.4.3 When an individual asks the College to restrict its processing of their Personal Data, the College is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

**4.5 Right to Data Portability**

4.5.1 Individuals have the right to obtain from the College a copy of their own Personal Data in a structured, commonly-used and machine-readable format (such as CSV files). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

4.5.2 The right to data portability only applies when:

- the individual provided the College with the Personal Data;
- The processing the College is carrying out is based on the individual's consent or is necessary for the performance of a contract; and
- the processing is carried out by automated means.

4.5.3 This means that the right to data portability does not apply to personal data the College is processing on another legal basis, such as its legitimate interests.

4.5.4 The College is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex provided that the College explains to the individual why it needs more time).

4.5.5 . The individual also has the right to ask the College to transmit the Personal data directly to another organisation if this is technically possible.

**4.6 Right to Object**

4.6.1 Individuals have the right to object to the College's processing of their Personal Data where:

- the College's processing is based on its legitimate interests or the performance of a task in the public interest and the individual has grounds relating to his or her particular situation on which to object;
- the College is carrying out direct marketing to the individual; and/or
- the College's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to his or her particular situation on which to object.

4.6.2 If an individual has grounds to object to the College's legitimate interests, the College must stop processing their Personal Data unless the College has compelling legitimate grounds for the processing which override the interests of the individual, or where the processing is for the establishment, exercise or defence of legal claims.

4.6.3 If an individual objects to direct marketing, the College must stop processing their Personal Data for these purposes as soon as the College receives the request. The College cannot refuse their request for any reason and cannot charge them for complying with it.

4.6.4 Before the end of one month from the date the College gets the request, the College must notify the individual in writing that the College has complied or intends to comply with their objections or that the College is not complying and the reasons why.

**4.7 Rights in Relation to Automated Decision Making**

4.7.1 Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is:

- necessary for entering into or performing a contract between the College and the individual;
- required or authorised by Data Protection Laws; or
- based on the individual's explicit consent

4.7.2 Automated decision making happens where the College makes a decision about an individual solely by automated means without any human involvement; and

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

4.7.4 The college does not currently use automated decisions or profiling, however, retains the right to, provided it adheres to the regulations in relation to this.

# 5. Related Documents

- Data Protection Policy
- Privacy Statement
- Breach Policy

- Data Retention Policy

Annex 1 Subject Access Request (SAR)/ Right of Access Request (RoAR) Procedure Flowchart