RIGHTS OF INDIVIDUALS POLICY

Author:	**Name**	Paris Bonwick	
	Job Title	Principal	
Date policy reviewed:	& 202	**Date policy to be reviewed**	D 202
GDPR Impact assessed by:	L. Farnhill	**Date impact assessed:**	&
Impact assessed by:	P Bonwick	**Date impact assessed:**	&
Policy approved by:	Corporation	**Date approved:**	th D 202

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 Education Group

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)

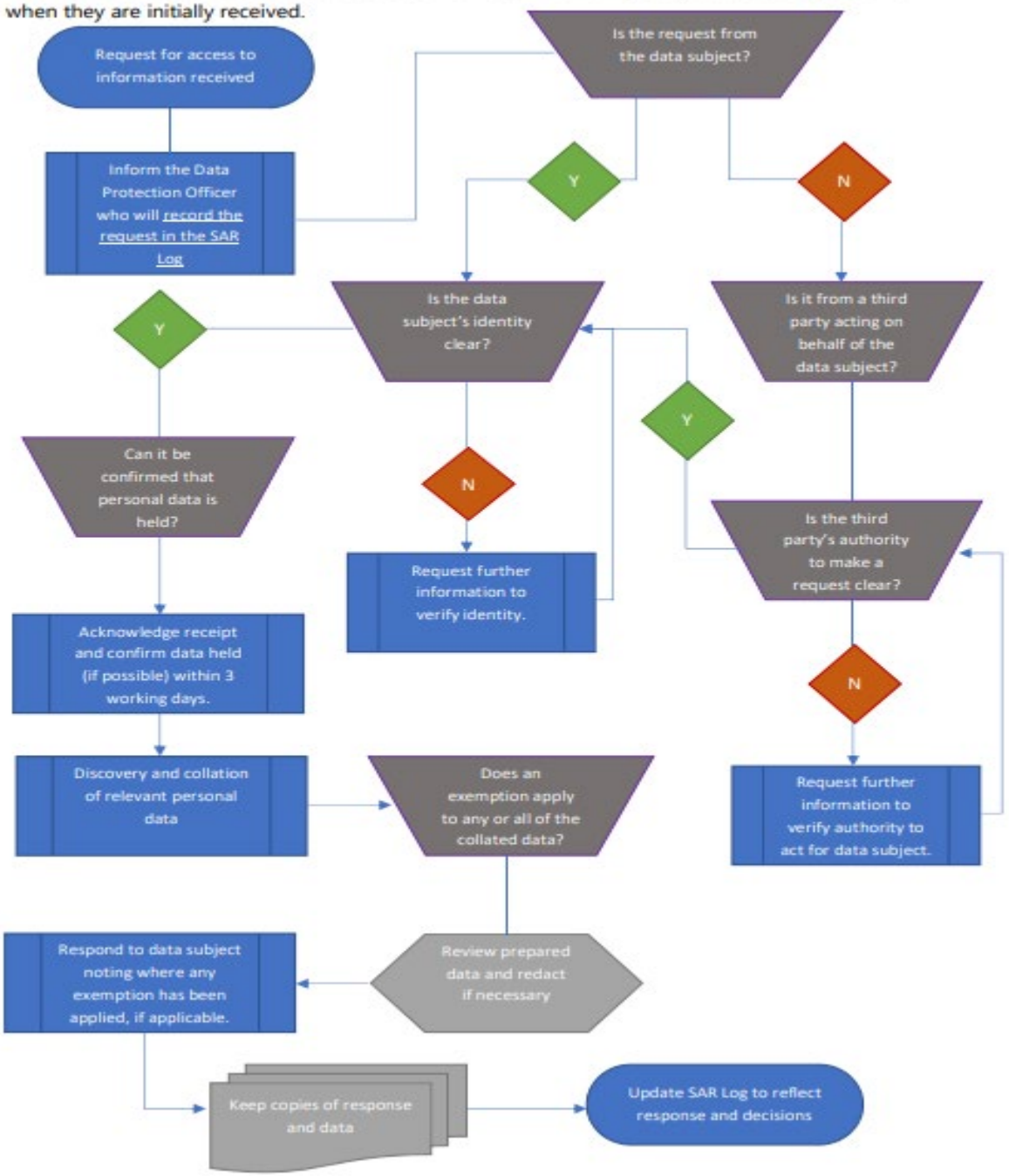
4.1.1 Individuals have the right to ask the College to confirm the Personal Data about them that the College is holding, and to have copies of that Personal Data along with the following information:

- 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.

Subject Access Request Procedure Flowchart

This flowchart describes the steps and decisions made in handling Subject Access Requests from when they are initially received.



Southport Education Group

Retention Policy

Author:	**Name**	Paris Bonwick	
	Job Title	Vice Principal Business Services	
Date policy reviewed:	February 2024	**Date policy to be reviewed**	March 2025
GDPR Impact assessed by:	L. Farnhill	**Date impact assessed:**	February 2024
Impact assessed by:	P Bonwick	**Date impact assessed:**	February 2024
Policy approved by:	Corporation	**Date approved:**	20th March 2024

1. INTRODUCTION

1.1 Southport Education Group (The "**College**") must, in respect of its processing of personal data, comply with the Data Protection Act 2018, the General Data Protection Regulation 2016/679, and related legislation (together, "Data Protection Laws").

1.2 This Retention Policy should be read in conjunction with the College's Data Protection Policy, which sets out the College's overall approach to data protection matters and sets out the rationale for why a Retention Policy is required for personal data.

1.3 The College is under a legal obligation to only to keep personal data for as long as the College needs it. Once the College no longer needs personal data, the College must securely destroy it. The College recognises that the correct and lawful treatment of data will maintain confidence in the College and will provide for a successful working environment.

1.4 This Policy applies to all College employees, consultants, contractors and temporary personnel hired to work on behalf of the College ("College staff").

1.5 All College Staff with access to personal data must comply with this Retention Policy.

1.6 Please read this Retention Policy carefully. All College Staff must comply with it at all times. If you have any queries regarding this Retention Policy, please consult your manager and/ or the Data Protection Officer. You are advised that any breach of this Retention Policy will be treated seriously and may result in disciplinary action being taken against you.

1.7 College Staff 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.

2. ABOUT THIS POLICY

2.1 This Retention Policy explains how the College complies with our legal obligation to only keep personal data for as long as we need it and sets out when different types of personal data will be deleted. In particular, it sets out details of the College's policies for the retention of Special Category personal data.

3. DATA RETENTION PERIODS

3.1 The College has assessed the types of personal data that the College holds and the purposes the College use it for.

3.2 Data broadly falls into two categories:

3.2.1: Data that must be retained for a set period, due to regulatory or organisational requirements as outlined in the table below

3.2.2: Data that has no fixed retention schedule (regulatory or organisational) and therefore must only be retained as long as it is necessary. Individuals and department are required to regularly review and destroy data that falls into this category. (Regular meaning no less than annual).

3.3 The table below sets out the retention periods for different types of data. It is the responsibility of the relevant department to ensure the data they hold is maintained for the period specified and securely destroyed at the end of the retention period.

3.4 Where years are stated below this refers to academic year not including the current year. For example in data with a retention period of 7 years from 2017/18 academic year would be destroyed after the 31st July 2025 (end of 2024/25).

3.5 If any member of College Staff considers a category of data needs to be kept for more or less time than the period set out in this policy, please contact the Data Protection Officer for guidance.

4. RETENTION PERIODS FOR DIFFERENT CATEGORIES OF DATA

4.1 Staff

File Description	Retention Period
Recruitment and selection – job application form and all aspects of recruitment and selection	Last action on application + maximum of 1 Year
Speculative job applications and CVs	Last action on application + maximum of 1 Year
Statistical information on profile of job applicants	5 Years
Personal details	6 years following termination of employment
Overtime records	6 years following termination of employment
Bank account details	6 years following termination of employment
Evidence of right to work in the UK	6 years following termination of employment
DBS information, list 99 and prohibition orders	6 years following termination of employment
Car insurance details	6 years following termination of employment
Requests for references	6 years following termination of employment
Certificates, qualification correspondence	6 years following termination of employment

Register of interests	6 years following termination of employment/governorship
Training and CPD records including development requests	6 years following termination of employment/governorship
Performance appraisal forms and correspondence	6 years following termination of employment
Discipline case files	6 years following termination of employment/last action on file
Staff records of an investigation that has a significant element of an allegation or report of abuse	until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer
Grievance case files	6 years following termination of employment/last action on file
Settlement agreements, COT3 and employment tribunal correspondence	6 years following termination of employment/last action on file, if Legal action taken, retain for the life of Institution
Performance management case files	6 years following termination of employment/last action on file
Lesson observation assessment data	6 years following termination of employment/last action on file
Trade Union correspondence	20 years following termination of employment/last action on file
Subject Access and Freedom of Information requests	2 years following last action unless longer retention requirements apply (i.e. H&S, Employment Law)
Allegations against a member of staff of a sexual nature.	Until the conclusion of the IICSA report. Thereafter, in line with the harm threshold: until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer
Allegations against a member of staff meeting the 'harm threshold'	until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer
Low level concerns raised by staff or students in relation to staff conduct with students (concerns that do not meet the 'harm threshold')	until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer

4.2 Health and Safety

Where there is a Statutory requirement to keep records for a specified period, it is recommended that the latest edition of the relevant legislation is checked and / or local Health and Safety Advisers

are consulted before disposing of other similar records. Examples of legislation with retention stipulations include:

a. Control of Substances Hazardous to Health Regulations;

b. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations;

c. Ionising Radiations Regulations;

d. Control of Lead at Work Regulations;

e. Control of Asbestos Regulations;

f. Work in Compressed Air Regulations; and

g. Social Security (Claims and Payments) Regulations

File Description	Retention Period
Accident records	3 years
Staff Health and safety records (i.e. PEEPs/Maternity risk assessment)	6 years following termination of employment
Student Health and safety records (i.e. PEEPs/Maternity risk assessment) Student Health and safety records linked to personal risk.	At end of academic year in which the programme ends 40 Years from date of document.

4.3 Financial Management

File Description	Retention Period
Finance System record (Accounts Payable, Accounts Receivable & General Ledger)	7 years
Bursary (Discretionary support) applications	7 years
Southport College Bank account	7 years
Supplier and customer correspondence	7 years

4.4 Student Records

File Description	Retention Period
Core student record	Lifetime of Student or 80 Years
MIS student record	7 years
Enrolment form	Termination of the student relationship plus 6 years
Application form	Termination of the student relationship plus 6 years
Interview sheet	Termination of the student relationship plus 6years

Copies of certificates	Termination of the student relationship plus 6 years
Pro-Monitor	Termination of the student relationship plus 6years
Team tracking	Termination of the student relationship plus 6 years
One-File	Termination of the student relationship plus 6 years
Disciplinary record (with no Safeguarding elements)	Termination of the student relationship plus 6 years
Student Disciplinary records of an investigation that has a significant element of an allegation or report of abuse	Date of Birth plus 25 Years; Looked After Children (LAC) records is currently Date of Birth plus 75 Years.
EHCP	7 years
Learners' portfolios and course work	12 weeks after receipt of certification
Internal verification documentation, along with the assessment tracking and feedback	3 Years after certification

4.5 Child Protection

File Description	Retention Period
Safeguarding record (Risk factors recorded for students)	Date of Birth plus 25 Years; Looked After Children (LAC) records is currently Date of Birth plus 75 Years.
Child Protection file if student completes at college and does not move to another provider	Date of Birth plus 25 Years; Looked After Children (LAC) records is currently Date of Birth plus 75 Years.
Receipt of Child Protection file if student moves to another provider and record is sent on as required by law	Date of Birth plus 25 Years; Looked After Children (LAC) records is currently Date of Birth plus 75 Years.
CSE records	Date of Birth plus 25 Years; Looked After Children (LAC) records is currently Date of Birth plus 75 Years.
Child In Need and social care interventions	Date of Birth plus 25 Years; Looked After Children (LAC) records is currently Date of Birth plus 75 Years.

4.6 Property

File Description	Retention Period
CCTV	Maximum of 31 days unless part of an investigation
Project Management Documents (e.g. PIDs, project plans etc.)	6 years
Routine planned preventative maintenance schedule checklists	Retain from year records created for 6 years
Records documenting assessments made to determine the presence (or presence) of asbestos in premises, as	Permanent Retention

required by Regulation 4(3) of the Control of Asbestos Regulations 2006 (SI 2006/2739).	
Records documenting the monitoring of the condition of asbestos in premises, and of maintaining or removing it.	Permanent Retention
Masterplans for sites & buildings & Deeds	Permanent Retention

4.7 Governance

File Description	Retention Period
Governors' records including contact details, register of interest and payments, photos & videos	6 years after the year in which the person ceases to be a governor
Minutes of meetings of the Corporation and its Committees, containing names of attendees	Life of institution
Records documenting the establishment and development institution's governance structure and rules.	Life of Institution
Establishment and Closure of Committees	Committee end date plus 6 years

4.8 There may be instances that require data to be retained longer than the stated period above. These exceptions will only be applied if retention can be justified on an operational or regulatory or statutory basis with the agreement of the Data Protection Officer.

5. DATA DISPOSAL

5.1. At the end of its retention period, data must be deleted/destroyed. Destruction of confidential information should be carried out in such a way that it cannot be recovered or reconstructed.

5.1.1. Non-sensitive paper information, that has no personal data (e.g. building risk assessments or learning materials) can be disposed of using recycle bins where appropriate

5.1.2. Confidential/sensitive information containing any personal data **CANNOT** be placed in an ordinary bin or recycling and must be made 'unreadable and un-reconstructable'. Government guidance outlines the following appropriate methods:

5.1.2.1. paper records should be shredded using a cross-cutting shredder or shredded by an external company.

5.1.2.2. CDs / DVDs / floppy disks should be cut into pieces

5.1.2.3. audio / video tapes and fax rolls should be dismantled and shredded

5.1.2.4. hard disks should be dismantled and sanded

5.1.3. College staff are asked to contact the IT team for support with the destruction and deletion of digital records and within IT equipment

5.1.4. The college uses a waste management contractor to destroy confidential paper

records securely and compliantly. Please ensure confidential paper records are placed in the confidential waste bags/boxes as supplied by the college's contractor

5.1.5. Staff are responsible for ensuring confidential waste sacks and boxes are kept in a secure locked location until collection

5.2. It is not necessary to document the disposal of records which appear on the Disposal Plan. Records disposed of outside of the Plan, for example by being disposed of earlier or kept for longer will need to be recorded for audit purposes.

6. SHARING

6.1. Copies of records should be destroyed when no longer required for the purpose they were copied. Where information has been regularly shared between departments, only the original records should be retained

6.2. Where the College shares information with other organisations, we must ensure they have adequate procedures for records to ensure that the information is managed in accordance with our policies, as well as current legislative and regulatory requirements.

6.3. Where appropriate we may carry out a data privacy impact assessment ahead of sharing data outside of the organization.