DATA PROTECTION
POLICY

Reviewed: September 2024

Next Review: September 2026

PETER SYMONDS COLLEGE	POLICY

Data protection policy

Contents

……

1. Aims

Peter Symonds College aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection

Regulation (UKGDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the UKGDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UKGDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The College processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The College is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by the College, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing body

The governing board has overall responsibility for ensuring that the College complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on college data protection issues.

The DPO is also the first point of contact for individuals whose data the College processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The College's DPO is Stephen Cowling and he is contactable via psc@psc.ac.uk .

5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the College of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that the College must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the College aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the College can **fulfil a contract** with the individual, or the individual has asked the College to take specific steps before entering into a contract
- The data needs to be processed so that the College can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the College, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the College or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the College's retention policy

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a member of staff, student or parent/carer that puts the safety of our staff or students at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted, either in writing or by email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Students and subject access requests

Personal data about a student belongs to that student, and not the student's parents or carers. For a parent or carer to make a subject access request with respect to a student for whom they have parental responsibility, the student must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Most subject access requests from parents or carers of students at the College will not be granted without the express permission of the student.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the student is at risk of abuse, where the disclosure of that information would not be in the student's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the student

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Freedom of Information requests

Anyone has the right to make a Freedom of Information request of a public authority. Freedom of Information requests to the College should be directed to the DPO either in writing or by email. Any member of staff receiving a Freedom of Information request should pass this immediately to the DPO.

The College will respond to Freedom of Information requests within 20 working days. It will either provide the information requested or give details of why, under the provisions of the Freedom of Information Act, it is unable to provide the information requested.

If all or part of the information requested cannot be provided, the person making the request will be informed:

- That they may request an internal review of the decision. To do this, they should contact the Principal (principal@psc.ac.uk). The Principal will direct a member of SMT not involved in the original decision-making to review the request and the decisions made.
- That, if they remain dissatisfied after internal review, they may contact the ICO.

11. Biometric recognition systems

Currently, the College does not make use of biometric recognition systems for students. If the College does decide to introduce such systems we will comply with the requirements of the Protection of Freedoms Act 2012.

Where staff members or other adults use the College's biometric system(s), we will obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the College will delete any relevant data already captured.

11. CCTV

We use CCTV in various locations around the college site to ensure it remains safe. We adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

12. Photographs and videos

From time-to-time, the College takes photographs or records video of students, staff, parents and visitors. These images and recordings are used in a variety of ways including:

- On internal display boards.
- On the College website.
- In the College prospectus.
- On College social media accounts.

The College does this with the lawful basis of carrying out a public task, namely the provision of education.

Students and staff have the right to object to the taking and use of their photograph, or the recording of video of them, by the College. They can do this by:

- Moving out of shot when a photograph or video is being taken on behalf of the College. Those taking photographs on behalf of the College will always allow this option.
- Contacting the DPO (psc@psc.ac.uk) if they wish to object to the use of a specific photograph or video of them.

Staff and students will be made aware of the College's policy on photography and video when they join the College, and parents will be informed when they create a Parent Portal account. Information about this policy will be provided to visitors on arrival in College. A reminder of the policy on photography will be provided to students and staff at the start of each academic year.

The College recognises that some photographs and video used for marketing purposes are highly visible for a sustained period of time. Students who are photographed for the prospectus will be asked to complete a form, at the time the photograph is taken, confirming that they do not object to its use in marketing materials.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our College and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- . Portable electronic devices, such as laptops and hard drives that contain personal data, are protected by password access control
- Staff are directed to ensure that papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Network configuration ensures that passwords that are at least 8 characters long containing letters and numbers are used to access College computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Staff are reminded regularly through training about good practice when using IT systems as as to avoid data breaches.
- Staff or governors who store personal information on their personal devices are expected to follow the same security procedures as for college-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the College's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The College will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a College context may include, but are not limited to:

- An email containing personal data being sent to the wrong recipient.
- A non-anonymised dataset being published on the College website which shows the exam results of individual students eligible
- Safeguarding information being made available to an unauthorised person
- The theft of a college laptop containing non-encrypted personal data about students

17. Training

All staff and governors are provided with data protection training as part of their induction process. A Data Protection training update is provided for all staff each September.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every 2 years** and scrutinized by SMT and the Audit Committee, prior to approval by the Governing Body.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- CCTV policy

- Privacy notices

20. About this policy

Does this notice impact on equal opportunities within the College? No

If so, give details and, if appropriate, indicate how these will be ameliorated.

Created: 30 March 2018

For review by the Data Protection Officer

Reviewed: September 2019 (No changes)
Reviewed: August 2020 (minor change)
Additional review: March 2021 (amalgamation of policy and key appendices)
Reviewed: September 2022
Review date: September 2024

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will notify the Principal of any data breach which needs to be reported to the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO.

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out: o The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects

  Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored by the College's Corporate Services Officer.

Actions to minimise the impact of data breaches

We will take action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Appendix 2: Retention of Data and Disposal of Data

Personal information should not be retained beyond its useful time. The College will archive and store 'formal records' held in central files for the periods of time indicated below. Other caches of data maintained by staff should either be added to the 'formal records' or be destroyed within two years of the subject (staff or student) leaving the College.

Student Data

In general, student 'formal records' will be kept for a maximum of **seven years** after they leave unless there are specific requests from the data subject to keep information for longer.

This will include:

- name, address and contact details
- date of birth, health and ethnicity details
- academic progress records, including attendance, coursework marks, exam achievements, pastoral records, access arrangements and disciplinary matters
- copies of academic/employment references

Examinations Data

A copy of the examination results for every student is held by the examinations office in perpetuity.

Applicant Data (paper based or online)

For those individuals who apply to the College but do not take up a place, data will be retained for 6 months after start of the academic year after the application was received by the College.

Staff Data

In general, staff information will be kept for **seven years** after the end of the academic year in which a member of staff leaves. Some information however will be kept for much longer – this includes information necessary in respect of pay, pensions, taxation, safeguarding concerns, potential or current disputes or litigation regarding the employment, and key information required for job references. We will retain basic terms of service and pensions records for **forty years** after a member of staff leaves. There are categories of data where health and safety legislation requires the retention of records for forty years, and where a member of staff has been subject to a safeguarding allegation personnel records are held indefinitely.

Applicant data (paper based or online)

Paperwork about unsuccessful job applicants will be kept for a maximum of six months after the end of the academic year in which the application was made.

Disposal Procedures

It is essential that personal data is disposed of correctly at the end of the relevant retention period. With the exception of student files which are scanned and disposed of off-site, paper records are archived on site for the appropriate retention period. At the close of this period, materials are passed to a certified waste contractor employed to shred or incinerate the material.

Computer records and files should be erased or rendered inaccessible in line with the retention policy. From a practical point of view records will be held on computer backup media for some considerable time (for example until the magnetic tapes are destroyed) but these data sets are only available to specialist personnel for the purposes of restoring selected data to 'Live' status in the event of system malfunctions; they are not available for general purposes.

Figure 1.0 details the retention periods for specific types of data. In practice, the retention period for most data is harmonised at seven years.

Figure 1.0 Retention periods for particular data

Type of Data	Detail Examples	Retention Period	Legislative context
Corporation and Executive Committee meetings	Minutes of meetings	Current year + 50 years	

Strategic Planning & Performance	Minutes of meetings	Current year + 10 years	
Insurance records	Certificates of insurance	Commencement or renewal of Policy date + 40 years	S.I. 1998 / 2573 Employer's Liability (Compulsory Insurance) Regulations 1998
Finance and Audit records	As advised by funding agencies and internal and external auditors	Current year + 6 years	c.58 Limitation Act 1980 / Various - Companies Acts
Medical records kept by reason of the control of substances hazardous to health	Personnel files and software	40 years after date of last entry	COSH Personnel 1999 & 2002
Medical records relating to asbestos	Personnel files and software	40 years after date of last entry	Control of Asbestos at Work Regulations 2002, 2006 & 2012
Medical records relating to ionising radiation	Personnel files and software	50 years or until person reaches 75 (the longer)	Ionising Radiations Regulations 1999
Medical records relating to an employee placed under surveillance for other health reasons	Personnel files and software	40 years after date of last entry	Management of Health & Safety at Work Regulations 1999
Student Records including academic achievements and conduct	• Course Work • Disciplinary Files • Enrolment Records • Achievement records • Attendance records • Learner Support files	7 years after the end of the academic year in which a student left the College	Limitation period for negligence
Personnel Files:	Personnel files and software	7 years from the end of the academic year in	Provision of references and limitation period for litigation

Type of Data	Detail Examples	Retention Period	Legislative context
Training records; notes of grievance, disciplinary and capability hearings		which the employment ended	
Staff Application Forms: Interview notes for those not appointed	Personnel files and software	6 months after the end of the academic year in which the application was made	Limitation period for litigation and reporting period
Facts relating to redundancies	Personnel files and software	7 years from the end of the academic year in which the events occurred	Limitation period for litigation

Income Tax and NI returns; correspondence with Tax Office	Personnel files and software	3 years after the end of the financial year to which the records relate, except for that in the Personnel file	Income Tax (Employment) Regulations 1993 as amended 1996
Statutory Maternity Pay	Personnel files and software	3 years after the end of the financial year to which the records relate, except for that in the Personnel file	Statutory Maternity Pay (General) Regulations 1986 as amended
Wages and salary records	Personnel files and software	7 years from the end of the academic year in which the employment ended, with the exception of basic data which is retained for 40 years	Taxes Management Act 1970 and National Minimum Wage Act 1998
Working time records	Personnel and departmental files and software	7 years from the end of the academic year in which the employment ended	Working Time Regulations 1998
Health Records	Personnel files and software	7 years from the end of the academic year in which the employment ended	Management of Health & Safety at Work regulations
Health Records where reason for termination of employment is concerned with health	Personnel files and software	7 years from the end of the academic year in which the employment ended	Limitation period for personal injury claims
Records of tests etc under COSHH	Department records	5 years from test	COSHH Regulations 1999 & 2002
Records of safeguarding allegations against staff unless found to be malicious	Personnel files	Indefinitely	Advice from Hampshire LADO
Student safeguarding records	Confidential records system files relating to at-risk students	Indefinitely (unless student transfers to a different provider, where the file follows the student)	Advice from Hampshire LADO
Internet filtering and monitoring records	Details of activity 'flagged' by the internet filter	Current academic year	Decision by SMT

Careers contacts	Contact details for Careers Department links	Five years from last active contact from data subject	Those on the Careers Contact register have been added on the basis of consent, and so that a register of links can be held by the Careers team. A retention period of five years is reasonable and appropriate for the purpose.

Appendix 3: Archiving Procedures

Where possible, all records should be held electronically. Student paper files are scanned, and the originals securely disposed of. Where it is necessary to retain paper files for the periods identified in the retention and disposal schedule, the following procedure is used. Only records which follow the standard 'seven year' retention periods should be archived in this way. Records with non-standard retention periods should be held by the department concerned.

Preparation

- Archiving boxes can be provided by the Estates Department but should be ordered in advance (preferably, two-weeks' notice is required).
- Records, files and documents to be archived in a logical manner which should allow quick and easy referencing.
- All hard-backed folders e.g. lever arch files and any re-usable or bulky items should be removed – where necessary, use recyclable brown bags/envelopes.
- All plastic wallets, large paperclips and bulldog clips etc should be removed.
- Pack into archiving boxes retaining alphabetical order and ensuring only one academic end year of records per box. Boxes should be full but not over full.
- Complete the **Record of Contents** form below and make sufficient copies to be able to place one copy on top of the packed records, one to be waterproofed & attached to the outside end of the box, one copy to be held by Estates and any copies you may require for future reference.

Storage

- Contact Estates Department who will check your Archives to ensure they comply with the above.
- Boxes will then be relocated to the Archive store for storage.
- Access to the Archive store can be arranged through the Estates Department only.

Destruction of Archives

- At the date specified on the archive form the Estates Department will arrange for the relevant archives to be correctly destroyed in accordance with current regulations.
- The date of disposal will be recorded on the **Record of Content** and held on file in the Estates Department.

RECORD OF CONTENTS

Department Name:	Academic Year Ending:	Destroy Date:
Name / role of person who prepared this box:		
Summary of contents		

Detail of contents (if appropriate)	Detail of contents (if appropriate)

Record of disposal	
Date of Disposal	**Name and signature of member of estates team**

Appendix Four: data protection impact assessments (PDIAs)

When the College makes significant changes to its operations which may carry a high risk in terms of implications for personal data, it must complete a data protection impact assessment using the following template. If an individual feels a DPIAmight be necessary, they should discuss it with the Data Protection Officer in the first instance.

Once completed, a Data Protection Impact Assessment will be scrutinised and agreed by the College's SMT. It will be kept on record by the Secretariat team, and reviewed on a two-yearly cycle.

Data Controller: Peter Symonds College
Data Protection Officer:
Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals concerned? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for the College, and more broadly?

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk above				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**

		Eliminated reduced accepted	Low medium high	Yes/no
Sign off				
DPO advice provided on/by:				
Referral to ICO Made yes/no:				
Summary of DPO advice:				
Review arrangements:				