Data Protection Policy

Originator	Director of MIS and Funding
Date of Last Approval	December 2025
Approval/review	College Executive Board
Review interval (years)	3
Date of next review/approval	December 2028
File Location	College website

C O N T E N T S

1. Purpose

1.1 South Bank Colleges (trading as Lambeth College) is committed to transparency in how it collects, uses, and protects personal data relating to its workforce and students. This policy outlines the College's obligations under data protection law and sets out individual rights and responsibilities.

1.2 This policy applies to:

- Personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices, and former employees (HR-related personal data).
- Personal data of students.

1.3 The College has appointed Claudia Forbes as its Data Protection Officer (DPO). The DPO advises on compliance and can be contacted at dataprotection@southbankcolleges.ac.uk.

1.4 Any questions about this policy or requests for further information should be directed to the DPO.

1.4 Questions about this policy, or requests for further information, should be directed to the data protection officer.

2. Definitions

2.1 **Personal data**: Any information relating to an identifiable individual. Processing includes collecting, storing, amending, disclosing, or destroying data.

2.2 **Special category data**: Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic data, and biometric data (used for identification).

2.3 **Criminal records data**: Information about criminal convictions, offences, allegations, and proceedings.

2.4 "**The College**" refers to Southbank Colleges throughout this policy.

3. Data protection principles

3.1 The College processes personal data in accordance with the following principles:

- Lawfully, fairly, and transparently.
- For specified, explicit, and legitimate purposes.
- Limited to what is necessary for processing.
- Accurate and kept up to date; inaccuracies are corrected or deleted promptly.
- Retained only for as long as necessary.
- Secured against unauthorised or unlawful processing, accidental loss, destruction, or damage.

3.2 Individuals are informed of:

- The purpose and legal basis for processing.
- How their data will be used, via privacy notices.

3.3 Processing of special category or criminal records data is carried out only where necessary for employment law obligations and in line with relevant policies.

3.4 Personal data is updated promptly when individuals notify changes.

3.5 HR-related personal data is stored in personnel files (hard copy or electronic) and HR systems. Retention is normally six years post-termination.

3.6 The College maintains records of processing activities in compliance with UK GDPR and the Data Protection Act 2018.

4 Individual rights

4.1 Under the UK General Data Protection Regulation (UK GDPR), individuals (data subjects) have the following rights regarding their personal data:

1. **Right to be informed** – To know how personal data is collected, used, and shared.
2. **Right of access** – To obtain a copy of personal data and supplementary information.
3. **Right to rectification** – To have inaccurate or incomplete data corrected.
4. **Right to erasure** ("right to be forgotten") – To request deletion of personal data in certain circumstances.
5. **Right to restrict processing** – To limit how data is used in specific situations.
6. **Right to data portability** – To receive personal data in a structured, commonly used, machine-readable format and transfer it to another controller.
7. **Right to object** – To object to processing based on legitimate interests or direct marketing.
8. **Rights related to automated decision-making and profiling** – To safeguard against decisions made solely by automated means that significantly affect individuals.

These rights are **not absolute** and may be subject to conditions set out in UK GDPR and ICO guidance.

More detail on each of these individual rights can be found in the ICO's guidance on the UK General Data Protection Regulation (UK GDPR) at:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

5 Subject access requests (one of the above 8 individual rights in the UK GDPR)

5.1 Individuals have the right to request access to their personal data. When a SAR is made, the College will provide:

- The purposes for processing.
- Categories of personal data processed.
- Recipients or categories of recipients (including any transfers to third countries or international organisations).
- Retention periods or criteria for determining retention.
- Rights to rectification, erasure, restriction, or objection.
- Right to lodge a complaint with the ICO.
- Source of the data (if not collected directly from the individual).
- Details of automated decision-making, including profiling, and its significance.
- Safeguards for international transfers.

5.2 The College will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

5.3 If the individual wants additional copies, the College will charge a fee, which will be based on the administrative cost to the College of providing the additional copies. This is in line with clause 5.6 (below) and the ICO guidance referenced there.

5.4 To make a subject access request, the individual should send the request to the Data Protection Officer (to email: **dataprotection@southbankcollges.ac.uk**). In some cases, the College may need to ask for proof of identification before the request can be processed. The College will inform the individual if it needs to verify his/her identity and the documents it requires.

5.5 The College will normally respond to a request within a period of one month from the date it is received. In some cases and in line with relevant ICO guidance, the College can extend the time to respond by a further two months if the request is:

- complex; or
- the College has received a number of requests from the individual – this can include other types of requests relating to individuals' rights. For example, if an individual has made a SAR, a request for erasure and a request for data portability simultaneously.

The time extension here is calculated as three months from the original start date, ie the day the College receives the request, fee or other requested information. If the College decides that it is necessary to extend the time limit by two months, the College will write to the individual within one month of receiving the original request to tell him/her if this is the case and explain why.

5.6 In line with ICO guidance, in most cases the College cannot charge a fee to comply with a SAR. However, the College can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

5.7 **Requests for information about children** - in line with guidance on this point from the ICO, before responding to a SAR for information held about a child, the College should consider whether the child is

mature enough to understand their rights. If the request is from a child and the College is confident they can understand their rights, the College should usually respond directly to the child. The College may, however, allow the parent or guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf (Source: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/#fee).

6 **Other individual rights** (under the UK GDPR as summarised at section 4 above)

6.1 Individuals have a number of other rights in relation to their personal data, as set out earlier in this policy under section *'4 Individual rights'* (earlier).

6.2 To ask the College to take any of these steps, the individual should send the request to the Data Protection Officer (to email: **dataprotection@southbankcolleges.ac.uk**).

7. Freedom of Information (FOI) requests

FOI requests are separate to data protection, but in some cases there may be linkages to data protection where FOI requests are made to a public authority.

In line with guidance from the ICO, The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Public authorities include government departments, local authorities, the NHS, state schools, police forces, and Universities and Further Education (FE) Colleges.

Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

However, The Freedom of Information Act 2000 does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, the ICO advises that they should make a data protection subject access request.

8 Data security

8.1 The College takes the security of personal data seriously and implements robust **technical and organisational measures** to protect against:

- Loss, accidental destruction, misuse, or unauthorised disclosure.
- Unauthorised access, except by employees performing their duties.

Internal policies and controls include:

- Secure systems and password protection.
- Access controls based on job roles.
- Encryption and secure storage for sensitive data.

Where third parties process personal data on behalf of the College:

- They act under **written instructions**.
- They are bound by **confidentiality obligations**.
- They must implement appropriate security measures in compliance with UK GDPR.

9 Data Protection Impact Assessments

9.1 The College conducts DPIAs where processing is likely to result in high risk to individuals' rights and freedoms. DPIAs assess:

- The necessity and proportionality of processing.
- Risks to individuals.
- Measures to mitigate those risks.

Examples include new technologies, large-scale processing of sensitive data, or systematic monitoring.

10 Data breaches

10.1 If a personal data breach poses a risk to individuals' rights and freedoms, the College will:

- Report to the ICO within 72 hours of discovery.
- Record all breaches, regardless of severity.

10.2 If the breach is likely to result in high risk, affected individuals will be informed promptly, including:

- Likely consequences.
- Mitigation measures taken.

10.3 Staff discovering or responsible for a breach must:

- Complete the Personal Data Breach Reporting Form (see Appendix 2).
- Submit it immediately to the Data Protection Officer at Dataprotection@southbankcolleges.ac.uk.
- Provide any supporting documentation.

11 Employee responsibilities

Employees must:

- Keep their own personal data up to date (e.g., via self-service HR).
- Access only data they are authorised to use.
- Maintain confidentiality and security by:

- Following access control rules, do not disclose data except to individuals (whether inside or outside of the College) who have appropriate authorisation, and only for authorised purposes.
- Using password protection and secure storage.
- Avoiding removal of personal data or devices without encryption or security measures.
- Not storing personal data on local drives or personal devices.

Failure to comply may result in disciplinary action, including dismissal for serious breaches.

12. Children's personal data

• Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

• In line with relevant ICO guidance, an individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

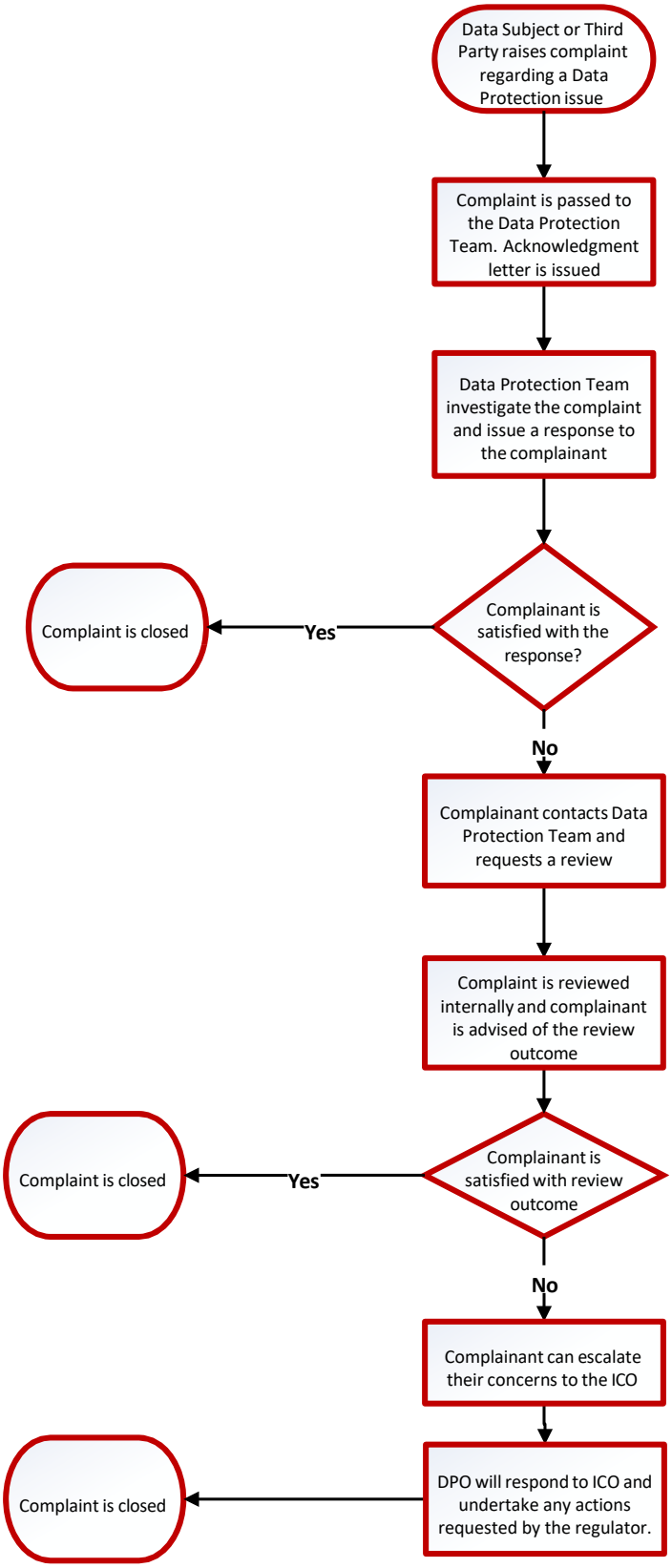
• More guidance on Children's personal data is available at:
https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/

13. Data Protection Complaints

Please see 'APPENDIX 1' (later) for the Data Protection Complaints procedure flowchart (summary flowchart).

Document dated: **28 November 2025**

APPENDIX 1 - Data Protection Complaints



Data Protection Complaints Procedure Flowchart (in summary)

Step 1 - Data Subject or Third Party raises complaint regarding a Data Protection issue.

Step 2 - Complaint is passed to the Data Protection Team. Acknowledgment letter is issued.

Step 3 - Data Protection Team investigate the complaint and issue a response to the complainant.

Step 4 - Complainant is satisfied with the response?

- **if yes, Complaint is closed.**

- **if no, Complainant contacts Data Protection Team and requests a review -** Complaint is reviewed internally and complainant is advised of the review outcome

- Complainant is satisfied with review outcome - **if yes, complaint is closed.**

- if no, Complainant can escalate their concerns to the ICO.

Step 5 **- DPO will respond to ICO and undertake any actions requested by the regulator** - **complaint is closed.**

APPENDIX 2 - Data Breaches

Personal data breach reporting form

Please provide as much information as possible and ensure that all fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please make it clear. In addition to completing the form below, please provide any other documentation relevant to the reported incident.

When the staff member (or their line manager) concerned who is responsible for the personal data breach (or who has discovered it) has completed this form, it should be returned asap to the Data Protection Officer of Lambeth College (to email**: dataprotection@southbankcolleges.ac.uk).**

In the wake of a personal data breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

In which Department did the breach take place?
What are the contact details of the individuals involved in the breach (individual(s) responsible for the breach/manager etc.) to discuss the incident being reported (Name and job title, email address, contact telephone number)

2. Details of the data protection breach

Describe the incident in as much detail as possible. When did the incident happen, how did it happen, how did you become aware of the breach, …			
Date of breach:		Date aware of breach:	
Type of breach (select one):	[Disclosure/Loss/Alteration/Destruction/Access]		

What/how much personal data was involved in the incident? Was any sensitive data involved, if so what?
How many individuals were affected?
Are the affected individuals aware that the incident has occurred? How did they become aware?
What are the potential consequences and adverse impacts on those individuals? What are the risks and how serious are they?
[Provide details, see guidance on assessing risks to individuals]

Likelihood of impacts/risks:	[None/unlikely/low/medium/high]

Have any of the affected individuals complained about the incident?

3. Containment and recovery

If there has been a delay in reporting the incident to the Data Protection Officer please explain your reasons for this.

Has the Department taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred. If not, please explain.

4. Steps to prevent recurrence

What steps has your organisation taken to prevent a recurrence of this incident?
What measures did the organisation have in place to prevent an incident of this nature occurring?
Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

5. Training and guidance

Lambeth College provides staff with data protection training. If so, please provide any extracts relevant to this incident here.

Data Protection training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?
Does your Department provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Miscellaneous

Has there been any media coverage of the incident? If so, please provide details of this.

(Unless it's a matter of urgency, please consult with the Data Protection Officer before any of the following actions)

Has the Information Commissioner or any other (overseas) data protection authorities been notified of this incident? If so, please provide details.
Has the Police been informed about this incident? If so, please provide further details and specify the Force(s) concerned.

Have any other regulatory bodies been informed about this incident? If so, please provide details.

APPENDIX 3 - Subject Access Requests (SARs)

In line with guidance from the ICO on SARs:

- Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- This is commonly referred to as a subject access request or 'SAR'.
- Individuals can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- Organisations should perform a reasonable search for the requested information.
- Organisations should provide the information in an accessible, concise and intelligible format.
- The information should be disclosed securely.
- Organisations can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

More information on Subject Access Requests (SARs) can be found at:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

and the ICO has also produced more detailed guidance on SARs at:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

-