Data Protection Policy

Date of Last Approval	29th June 2021
Date of Equality Impact Assessment	
Approval/review bod(ies)	CLG
Review internal (years)	3 Years
Date of next review/approval	28 June 2024
Evaluation	Ongoing
File Location	Online
Originator	Alistair Dunkwu – Director of MIS, Exams & Subcontracting

C O N T E N T S

Topic	Page
POLICY	
1 Purpose	3
2 Definitions	3
3 Data Protection Principles	3
4 Individual Rights	4
5 Subject Access Requests	5
6 Other individual rights	6
7 Freedom of Information (FOI) requests	6
8 Data Security	7
9 Data Protection Impact Assessments	7
10 Data Breaches	7
11 Employee Responsibilities	7
12 Children's personal data	8
13 Data Protection Complaints	8
Appendices	
APPENDIX 1 - Data Protection Complaints	9
APPENDIX 2 - Data Breaches	11
APPENDIX 3 - Subject Access Requests (SARs)	15

1. Purpose

1.1 South Bank Colleges (trading as Lambeth College), is committed to being transparent about how it collects and uses the personal data of its workforce and students, and to meeting its data protection obligations. This policy sets out Lambeth College's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 This policy applies both to:
(a) the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees - this is sometimes referred to as HR-related personal data; and
(b) this policy also applies to the handling of student data.

1.3 Lambeth College has appointed Alistair Dunkwu as its data protection officer. His role is to inform and advise Lambeth College on its data protection obligations. He can be contacted at email: **dataprotection@lambethcollege.ac.uk**

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"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2.2 **"Special categories of personal data"** means personal data concerning racial or ethnic origin, personal data revealing political opinions, personal data revealing religious or philosophical beliefs, personal data revealing trade union membership, data concerning health, data concerning a person's sex life, data concerning a person's sexual orientation, genetic data and biometric data (where used for identification purposes).

2.3 **"Criminal records data"** ('criminal offence data') means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

2.4 **"Lambeth College"** is hereinafter referred to as the College.

3. Data protection principles

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

- The College processes personal data lawfully, fairly and in a transparent manner.
- The College collects personal data only for specified, explicit and legitimate purposes.
- The College processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

• The College keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
• The College keeps personal data only for the period necessary for processing.
• The College adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

3.2 The College tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

3.3 Where the College processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

3.4 The College will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.5 Personal data gathered during the employment, worker, contractor or volunteer relationship, apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the College holds HR-related personal data is normally no longer than six years post termination.

3.6 The College keeps a record of its processing activities in respect of personal data in accordance with the requirements of the (now) UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018.

4 Individual rights

4.1 As a data subject, individuals have a number of rights in relation to their personal data.
The UK GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

These rights are not absolute, and are subject to certain criteria as set out for example in the ICO's UK GDPR 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 make a subject access request. If an individual makes a subject access request, the College will tell him/her:

- the purposes for processing;
- categories of personal data the College is processing;
- recipients or categories of recipient the College has or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- the retention period for storing the personal data or, where this is not possible, the criteria for determining how long the College will store it;
- the individual's right to request rectification, erasure or restriction or to object to processing;
- the individual's right to lodge a complaint with the Information Commissioner's Office (ICO);
- information about the source of the data, if the College did not obtain it directly from the individual;
- whether or not the College uses automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and
- the safeguards the College has provided where personal data has or will be transferred to a third country or international organisation.

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@lambethcollege.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 Lambeth College to take any of these steps, the individual should send the request to the Data Protection Officer (to email: **dataprotection@lambethcollege.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; it has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Where the College engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

9 Data Protection Impact Assessments

9.1 Some of the processing that the College carries out may result in data protection risks. Where processing would result in a high risk to individual's rights and freedoms, the College will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

10 Data breaches

10.1 If the College discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner's Office (ICO) within 72 hours of discovery. The College will record all data breaches regardless of their effect.

10.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

10.3 The staff member (or their line manager) concerned who is responsible for the personal data breach (or who has discovered it) should complete the 'Personal data breach reporting form' (**at *'APPENDIX 2 - Data Breaches'* of this policy**) as soon as possible. Once completed, it should be returned asap to the Data Protection Officer of Lambeth College (to email: **dataprotection@lambethcollege.ac.uk**). In addition to completing that form, the staff member should also provide any other documentation relevant to the reported incident.

11 Employee responsibilities

11.1 Individuals are responsible for helping the College keep their personal data up to date by ensuring they use self-service HR for example if an individual moves house or changes his/her bank details.

11.2 Employees may have access to the personal data of other employees and students in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the College relies on individuals to help meet its data protection obligations to staff and students.

11.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;

• not to disclose data except to individuals (whether inside or outside the College) who have appropriate authorisation;

• to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

• not to remove personal data, or devices containing or that can be used to access personal data, from the College's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

• Not to store personal data on local drives or on personal devices that are used for work purposes.

11.4 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the College's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

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.

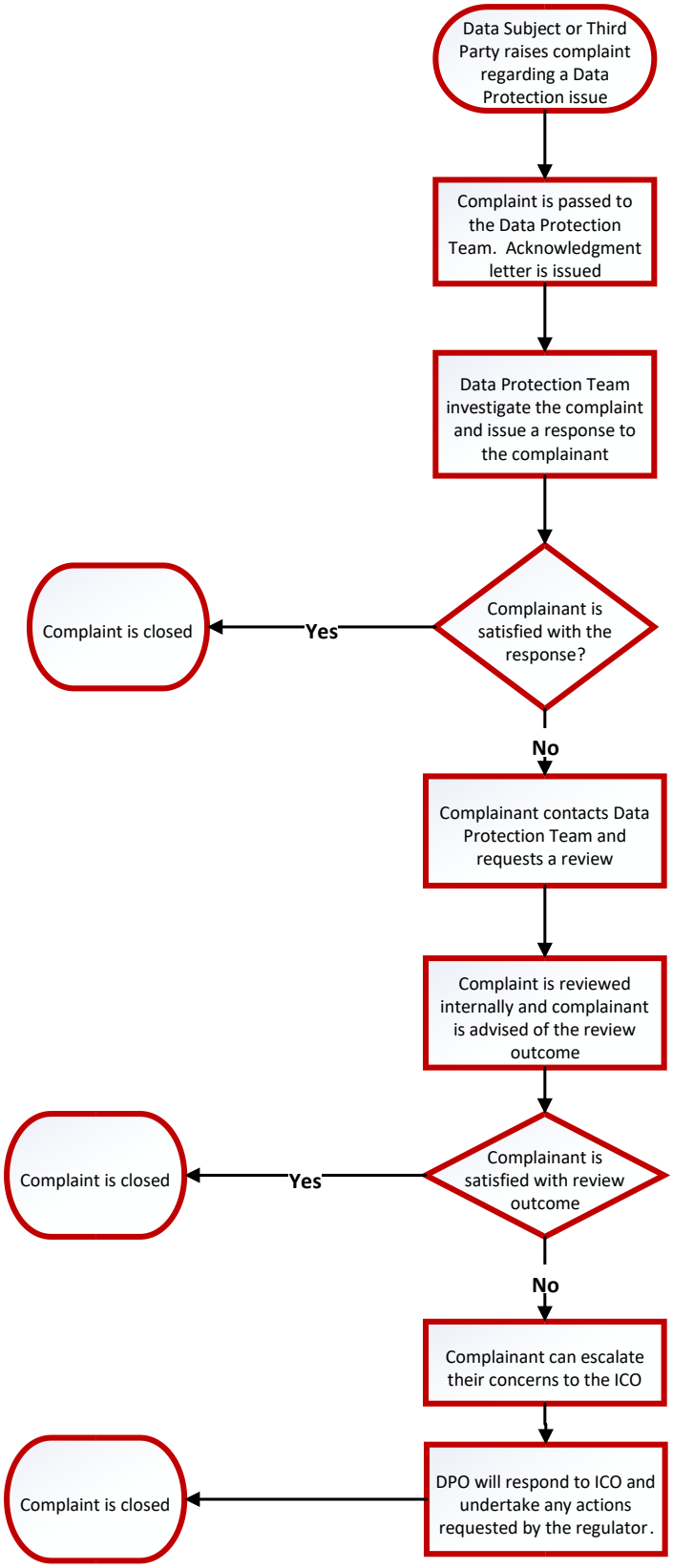
• More guidance on Children's personal data is available at:
https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/

13. Data Protection Complaints

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

Document dated: **20 June 2021.**

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@lambethcollege.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/

-