GDPR & Data Protection Policy

Policy owner: Zubair Ahmad

Final Review Date: July 2026
Next Review Due: July 2027

Address: 3rd Floor, 277 Cranbrook Road

Ilford, IG1 4TG

Tel: 0208 2617372

Email: info@londoncollege.co.uk

Web: https://londoncollege.co.uk

1. Purpose and Scope

AA London College is committed to protecting the privacy, rights and personal information of its learners, applicants, staff, alumni, visitors, partners and other individuals whose personal data it processes. This Policy explains how personal information is collected, used, stored, shared, retained and securely disposed of.

The Policy applies to all personal data processed by the College, whether held electronically, digitally, on paper or within another structured record system. It applies to all staff and authorised persons who collect, access, use, disclose or otherwise process personal data on behalf of the College.

The College will comply with applicable UK data protection and privacy legislation, including:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Privacy and Electronic Communications Regulations 2003, where applicable.

The Data (Use and Access) Act 2025 updates aspects of the existing UK data protection framework rather than replacing the UK GDPR or Data Protection Act 2018.

2. Definitions

Personal Data: Information relating to an identified or identifiable living individual.

Data Subject: The individual to whom personal data relates.

Processing: Any operation performed on personal data, including collecting, recording, organising, storing, accessing, using, sharing, altering, restricting, deleting or destroying it.

Special Category Data: Sensitive personal information including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, health information, sex life or sexual orientation.

Data Controller: The organisation that determines why and how personal data is processed.

Data Processor: A person or organisation processing personal data on behalf of a controller.

Third Party: A person, organisation or public body other than the data subject, controller, processor or authorised persons acting under their authority.

Personal Data Breach: A security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

Profiling: Automated processing used to evaluate, analyse or predict aspects relating to an individual.

Filing System: A structured set of personal data accessible according to specific criteria.

3. Data Protection Principles

The College will ensure that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as necessary.
- Protected by appropriate technical and organisational security measures.
- Managed in a way that allows the College to demonstrate compliance.

These principles reflect the core requirements already contained in the College's existing data protection arrangements.

4. Lawful Basis for Processing

Before processing personal data, the College will identify an appropriate lawful basis. Depending on the circumstances, this may include:

- Consent.
- Performance of a contract.
- Compliance with a legal obligation.
- Protection of vital interests.
- Performance of a task in the public interest.
- Legitimate interests, where appropriate.

Where special category data is processed, the College will identify both an appropriate lawful basis and an additional legal condition for processing.

Consent will only be relied upon where it is appropriate, freely given, specific, informed and capable of being withdrawn.

5. Personal Data Processed

The College may process information relating to:

- Applications, admissions and enrolment.
- Identity and contact information.
- Attendance and participation.
- Assessment, achievement and certification.
- Reasonable adjustments and special considerations.
- Employment and payroll.
- Fees and financial transactions.
- Health, welfare and safeguarding.
- Equality and diversity monitoring.
- Complaints, appeals and disciplinary matters.

- Website and online learning activity.
- IT system access and security.
- Regulatory and awarding body requirements.
-

Only information that is reasonably necessary for a legitimate purpose will be collected.

6. Privacy Information and Transparency

Individuals will be provided with appropriate information about how their personal data is processed.

Privacy information will normally explain:

- Who is collecting the information.
- Why the information is required.
- The lawful basis for processing.
- Who information may be shared with.
- How long it may be retained.
- Applicable individual rights.
- International transfers, where relevant.
- How to raise a complaint.
- Relevant automated decision-making or profiling.

Electronic and paper-based data collection forms should contain appropriate privacy wording or provide a link to the relevant privacy notice.

New data collection processes and systems should be reviewed to ensure that privacy information is provided appropriately. The existing policy already requires fair-processing information to accompany relevant data collection methods.

7. Data Accuracy and Minimisation

The College will take reasonable steps to ensure personal data is accurate, relevant and limited to what is required.

Staff must:

- Check information before recording it.
- Correct known errors promptly.
- Update records when relevant details change.
- Avoid collecting unnecessary information.
- Report known inaccuracies.

Learners, staff and other individuals should inform the College when their information changes.

Where inaccurate information has already been disclosed to a relevant third party, the College will provide corrected information where required.

The College will periodically review relevant data collection methods to ensure information remains adequate, relevant and proportionate.

8. Data Retention and Secure Disposal

Personal data will only be retained for as long as necessary for the purpose for which it was collected, or where continued retention is required for legal, regulatory, contractual, financial,

safeguarding, awarding body or other legitimate purposes.

Retention periods may vary according to the record type. For example:

- Learner registration and achievement records will be retained in accordance with awarding body and regulatory requirements.
- Assessment and internal quality assurance records will be retained for the applicable required period.
- Financial records will be retained in accordance with statutory requirements.
- Employment records will be retained in accordance with applicable employment and legal requirements.
- Safeguarding records will be retained in accordance with safeguarding requirements.
- Complaints and appeals records will be retained for an appropriate period according to the nature of the matter.
- Routine correspondence will be retained only for as long as reasonably necessary.

The Data Protection Officer/GDPR Owner will review retention arrangements periodically and identify information that is no longer required.

When retention periods expire, information will be securely disposed of through measures such as:

- Confidential shredding.
- Secure electronic deletion.
- Secure erasure or destruction of storage devices.
- Approved confidential waste arrangements.

Any retention beyond an established retention period must have a legitimate reason and, where appropriate, be authorised and recorded in writing. This retains the annual review and written-authorisation controls in the existing policy.

9. Sharing Personal Data With Third Parties

Personal data may be shared with third parties where there is a lawful, necessary and legitimate reason.

Recipients may include:

- Awarding bodies.
- Regulatory and government bodies.
- Funding bodies.
- Professional advisers.

- Accountants and auditors.
- IT and software providers.
- Payroll and financial service providers.
- Legal advisers.
- Emergency services.
- Safeguarding authorities.

Before sharing information, the College will consider:

- The lawful basis and purpose.
- Whether sharing is necessary and proportionate.
- The minimum information required.
- Whether the recipient is authorised.
- The recipient's security arrangements.
- Whether a data processing, confidentiality or data sharing agreement is required.

Personal data must not be disclosed to unauthorised persons.

Where an external organisation processes personal data on behalf of the College, appropriate written contractual arrangements will be used to require confidentiality, security, lawful processing and suitable controls. The College may conduct proportionate checks to obtain assurance of compliance.

The College's existing policy already requires appropriate confidentiality or data-sharing arrangements before third parties access College-held data.

10. International Data Transfers

Personal data will only be transferred outside the UK where permitted under applicable data protection legislation.

The College will consider whether:

- The destination benefits from UK adequacy arrangements.
- Appropriate contractual safeguards are required.
- Another recognised legal transfer mechanism applies.
- Additional protections are necessary.

The Data (Use and Access) Act 2025 introduced changes to aspects of the UK international transfer framework.

11. Cookies and Website Technologies

The College website and online services may use cookies or similar technologies for:

- Core website operation.
- Security and session management.
- User preferences and functionality.

- Website analytics and statistical measurement.

Cookies may include strictly necessary, functional and analytics cookies.

Where consent is legally required, non-essential cookies will not be placed until appropriate consent has been obtained.

Users will be provided with clear information about:

- Types of cookies used.
- Their purposes.
- How long they remain active.
- Whether third parties are involved.
- How cookie preferences can be managed or withdrawn.

The Data (Use and Access) Act 2025 allows certain limited low-risk storage and access technologies to be used without explicit consent where the relevant legal conditions are met.

12. Information Security

The College will implement appropriate technical and organisational measures to protect personal data from accidental or unlawful loss, destruction, alteration, disclosure or access.

Technical measures may include:

- Password protection and strong password controls.
- Automatic locking of inactive devices.
- Role-based access permissions.
- Multi-factor authentication where appropriate.
- Anti-virus, anti-malware and firewall protection.
- Encryption where appropriate.
- Restrictions on removable media.
- Secure networks and remote access.
- Secure backups.
- Pseudonymisation or anonymisation where appropriate.
- Periodic review of access rights.

Organisational measures may include:

- Staff training and confidentiality requirements.
- Physical access controls.
- Locked storage for confidential records.
- Secure handling of paper files.
- Restrictions on portable devices.
- Secure disposal procedures.
- Appropriate processor and supplier controls.

Staff must not access information without a legitimate business need, share passwords, leave confidential information unattended or disclose information to unauthorised persons.

The existing policy already includes password protection, locking terminals, firewalls, encryption, network security, access controls, secure storage, staff training and backups.

13. Individual Rights

Subject to applicable legal conditions and exemptions, individuals may have the right to:

- Be informed about processing.
- Access their personal data.
- Request correction.
- Request erasure in certain circumstances.
- Request restriction of processing.
- Object to certain processing.
- Request data portability where applicable.
- Withdraw consent where consent is relied upon.
- Challenge certain automated decisions.
- Make a data protection complaint.

14. Subject Access Requests

Individuals may request access to personal information held about them.

Requests may be made in writing or by email. The College may request sufficient information to confirm identity and locate the requested records.

The College will normally respond within one month, subject to any lawful extension.

The College will undertake reasonable and proportionate searches when responding to requests, reflecting the clarification introduced by the Data (Use and Access) Act 2025.

Requests will normally be handled free of charge unless a fee is lawfully permitted.

15. Rectification, Erasure and Restriction

Individuals may request correction of inaccurate or incomplete personal data.

Where appropriate, the College will:

- Correct information without undue delay.
- Update relevant records.
- Inform relevant recipients of corrections where required.
- Consider valid erasure requests.
- Restrict processing where legally required.

Information will not necessarily be deleted where the College must retain it for legal, regulatory, contractual, safeguarding or other lawful reasons.

16. Automated Decision-Making and Profiling

Where the College uses solely automated processing to make a decision that has legal or similarly significant effects on an individual, appropriate safeguards will be applied.

These may include:

- Providing relevant information about the process.
- Allowing the individual to make representations.
- Providing meaningful human intervention.
- Allowing the decision to be challenged.

The Data (Use and Access) Act 2025 amended the rules relating to significant automated decisions while retaining safeguards and additional restrictions in relation to certain sensitive data.

17. Data Protection Impact Assessments and Processing Records

The College will maintain appropriate records of its personal data processing activities where required.

Records may include:

- Purposes of processing.
- Categories of information and individuals.
- Recipients.
- Retention periods.
- International transfers.
- Security arrangements.
- Lawful bases.

A Data Protection Impact Assessment (DPIA) will be considered where proposed processing is likely to create a high risk to individuals, including significant new technology, systematic monitoring, large-scale sensitive data processing or significant automated decision-making.

DPIAs should identify the processing purpose, risks and controls required to reduce those risks before processing begins wherever practicable.

The existing policy already requires review of processing records and use of DPIAs as part of the College's accountability arrangements.

18. Personal Data Breaches

Any actual or suspected personal data breach must be reported immediately to the Data Protection Officer/GDPR Owner or senior management.

Examples include:

- Loss or theft of information.
- Unauthorised access.
- Information sent to the wrong person.

- Cybersecurity incidents.
- Accidental disclosure, deletion or alteration.

The College will:

- Record and assess the incident.
- Take appropriate containment action.
- Identify affected information and individuals.
- Assess potential harm.
- Determine whether notification to the Information Commissioner's Office is required.
- Notify affected individuals where legally required.
- Investigate the cause.
- Implement corrective or preventative action.

19. Data Protection Complaints

Individuals may complain if they have concerns about how the College has collected, used, stored, shared or otherwise processed their personal information.

Complaints may be submitted by email or in writing.

The College will:

- Provide an accessible complaints route.
- Acknowledge a data protection complaint within 30 days.
- Investigate it appropriately.
- Maintain a record of the complaint and outcome.
- Respond without undue delay.
- Explain further complaint rights where appropriate.

The DUAA complaints provisions came into force on 19 June 2026.

Where an individual remains dissatisfied, they may have the right to complain to the Information Commissioner's Office.

20. Responsibilities

Data Protection Officer / GDPR Owner

The Data Protection Officer/GDPR Owner is responsible for:

- Monitoring compliance.
- Providing data protection advice.
- Supporting individual rights requests.
- Maintaining or overseeing processing records.
- Supporting breach management.
- Advising on DPIAs.
- Reviewing retention arrangements.
- Supporting data sharing arrangements.
- Reviewing relevant security and privacy risks.

- Promoting good practice.

Managers

Managers are responsible for:

- Promoting appropriate information handling.
- Ensuring staff understand their responsibilities.
- Maintaining suitable access controls.
- Identifying and escalating data protection risks.

Staff

All staff who process personal data must:

- Follow this Policy.
- Maintain confidentiality.
- Access information only where authorised.
- Keep records accurate.
- Protect passwords and devices.
- Follow retention and disposal requirements.
- Report data breaches immediately.
- Complete relevant training.
- Seek guidance where uncertain.

The existing policy assigns data protection responsibilities to the Data Protection Officer/GDPR Owner, managers and all staff processing personal data.

21. Staff Training and Policy Breaches

The College will provide appropriate data protection and information security training according to staff responsibilities.

A serious, deliberate or negligent breach of this Policy may result in:

- Management action.
- Additional training.
- Restriction or removal of system access.
- Disciplinary action.
- Referral to appropriate authorities where legally required.

22. Monitoring and Review

Compliance with this Policy will be monitored through appropriate management oversight, record reviews, security checks, retention reviews, training monitoring and audits where appropriate.

The Policy will normally be reviewed annually or earlier where required because of:

- Changes in legislation or regulatory guidance.
- Changes in College systems or activities.

- New technologies.
- Significant data protection incidents.
- Audit findings or identified compliance risks.