LONDON
COLLEGE

IT POLICY

Policy Owner : Zubair Ahmad

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

Address: 3rd Floor, 277 Cranbrook Road,
IG1 4TG, Ilford, England

Email: info@londoncollege.co.uk

Web: https://londoncollege.co.uk/

1. Purpose

The purpose of this policy is to ensure AA London College maintains the highest standards of data protection in compliance with the **UK GDPR** and **Data Protection Act 2018**. It outlines the College's approach to safeguarding student and staff data on digital platforms, particularly Moodle**.**

2. Scope

This policy applies to:

- All College staff, students, and third-party service providers accessing or managing College data and systems.
- All usage of the Moodle Virtual Learning Environment (VLE).

3. Use of Moodle for Assignments

All student coursework, assignments, and learning materials must be submitted or accessed exclusively via **Moodle**.

4. Secure Access Controls

To protect personal and academic data, the following security measures are enforced:

- **Password Protection:** Strong passwords required per College standards.
- **Two-Factor Authentication (2FA):** Mandatory for all Moodle logins.
- **Google Login Integration:** Secure Google SSO for AA London College email accounts.
- **Automatic Logout:** Sessions auto-expire after inactivity to prevent unauthorised access.

5. Data Protection and Privacy

Compliance: All data processing follows GDPR principles—lawful, fair, and transparent.

Data Minimisation: Only necessary personal data is collected and stored.

Access Control: Role-based access ensures only authorised users can view or manage data.

Encryption: All data transmitted to and from Moodle is encrypted via HTTPS (SSL).

6. Responsibilities

IT Department: Maintains, secures, updates, and monitors Moodle for vulnerabilities.

Academic Staff: Upload, manage, and assess coursework in compliance with data protection standards.

Students: Safeguard login credentials and report suspicious activity immediately.

Data Protection Officer (DPO): Oversees compliance and investigates breaches or unauthorised access.

7. Breach Reporting

Any suspected or actual data breach must be reported immediately to the **IT** Helpdesk.

8. Policy Violations

Violations may result in disciplinary action, access suspension, or legal consequences depending on severity.

9. Review and Update

This policy will be reviewed annually or as required following changes in legal or technical standards.