IT Use 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/

Introduction

This policy has been formulated in response to HM Government Prevent Duty Guidance for Higher Education Colleges in England and Wales. This guidance was updated by the department and is the subject of the duty under section 26 of the Counter-Terrorism and Security Act 2015 which applies to specified authorities including schools and colleges. Considering the above, AA London College understands its role in safeguarding its learners, and for this it has a detailed Prevent Duty Policy available on the website and has also formed its IT Use Policy accordingly.

Use of IT facilities at the College is only allowed to learners or staff with restricted use and on the basis that they use these as per the College's requirements. The College also recognizes its duties under the Prevent requirement as detailed in our Prevent Policy. The aim of this policy is to help ensure that the IT facilities can be used safely, lawfully, and fairly. These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third-party services, online services, or IT credentials) provided by the College.

Use of IT Facilities

IT resources are provided primarily to facilitate a person's essential work as a staff member or student or other role within the College. No use of any IT service should interfere with another person's duties, studies, or any other person's use of IT systems, nor bring the College into disrepute in any way. Using College IT facilities in an office, library, or laboratory for non-work-related purposes, such as personal electronic mail or recreational use of the internet including social networking sites, is permitted to enhance the overall experience of a staff member or student but is not an absolute right. Priority must always be granted to those needing facilities for academic work or other essential College business. College e-mail addresses and associated e-mail systems must be used for all official College business, in order to facilitate auditability and institutional record-keeping. All staff must regularly read their College e-mail.

Behaviours

1. No person shall jeopardise the integrity, performance, or reliability of computer equipment, software, data, and other stored information. Users must take adequate precautions against malicious software, such as computer viruses and malware.
2. All users of IT services must ensure that any computer for which they have responsibility and which is attached to the College network is adequately protected against viruses, and reasonable care should be taken to ensure resource use does not result in a denial of service to others.
3. Conventional norms of behaviour apply to IT-based media, just as they would apply to more traditional media. Within the College setting, academic freedom will always be respected. The College is committed to achieving an educational and working environment which provides equality of opportunity and freedom from discrimination on the grounds of race, colour, nationality, ethnic origin, gender, gender identity, marital or civil partnership status, disability, including mental health difficulties, sexual orientation, religion or belief, age, social class, pregnancy, or background. Distributing material that is offensive, obscene, or abusive may be illegal and may contravene College's approach on harassment.
4. No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper. Users of external services are expected to abide by any policies, rules, and codes of conduct applying to such services. Any breach of such policies may be regarded as a breach of this Policy and dealt with accordingly. This includes social networking sites, blog and wiki services, and other externally hosted services.

Acceptable Use

The College will only allow legitimate and relevant use of the IT facilities. Acceptable use can be described as follows:

1. IT facilities are limited to relevant educational purposes in line with academic freedom.
2. Learners may conduct research or browse the internet only for educational purposes.
3. IT facilities cannot be used for irrelevant purposes such as Facebook or YouTube for non-educational use.
4. IT facilities cannot be used to promote marketing or advertising material by a learner for personal interest.
5. IT facilities cannot be used to access or promote explicit content.
6. IT facilities cannot be used to access or promote content related to radicalisation or extremism.
7. Retention or propagation of material that is offensive, obscene, or indecent is prohibited except during recognised research or teaching permitted under UK and international law.
8. Intellectual property rights, including copyright, trademark, patent, and design rights, must not be infringed.
9. No unsolicited advertising ("spamming").
10. No sending emails purporting to come from someone else using forged addresses.
11. No unauthorised resale of College services or information.
12. Actions or inactions that aid the distribution of viruses or malicious software are prohibited.
13. No publication of unauthorised recordings (e.g., lectures) on external websites.
14. No posting defamatory comments about staff or students on social networking sites.
15. Web content portraying official College business requires express permission.
16. Users must comply with current UK laws, including intellectual property law, the Computer Misuse Act 1990, data protection laws, the Regulation of Investigatory Powers Act 2000 (RIPA), and Counter-Terrorism and Security legislation.

Use of College Internet via College Computers and Learners' Personal Devices

Learners and staff must adhere to the College's acceptable use requirements. Any individuals found in breach will be subject to disciplinary procedures.

Use of College Portal

Learners must adhere to the College's acceptable use requirements when using the portal. Sharing of information or messages through the portal is also subject to these rules. Breaches will result in disciplinary procedures.

Monitoring and Control

The College will continuously monitor internet activity and portal usage by reviewing logs to detect any matters or activities that breach permitted IT use.