Acceptable Use of Information Technology Policy
Strategic Approaches

The College seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning, teaching and research, including business and community engagement partnerships. Whilst academic freedom will be respected, this also requires responsible and legal use of the technologies and facilities made available to students, staff and friends of the College.

This Policy is intended to provide a framework for such use of Alexander London College's
I.T. resources. It applies to all computing, telecommunication, and networking facilities provided at the College. It should be interpreted such that it has the widest application, references to I.T. services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of an I.T. service. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to.

Users of commercial broadband services provided, or facilitated by, the College must abide by any specific policies associated with those services. Members of the College and all other users of the College's facilities are bound by the provisions of these policies in addition to this Acceptable Use of IT Policy.
It is the responsibility of all users of Alexander London College's I.T. services to read and understand this policy.

Purpose of Use
College I.T. resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the College. Facilities are also intended to help enhance the wider experience of students attending the College. No use of any I.T. service should interfere with another person's duties or studies or any other person's use of I.T. systems, nor bring the College into disrepute, in any way.

Using College I.T. facilities in an office, library or laboratory, for non-work-related purposes, such as personal electronic mail or recreational use of the World Wide Web including social networking sites, are understood to enhance the overall

experience of an employee or student but are not an absolute right. Priority to such College-owned facilities must always be granted to those needing facilities for academic work or other essential College business.

College email addresses must be used for all official College business in order to facilitate auditability and institutional record keeping. All staff and students of the College must regularly read their College email.

Commercial work for outside bodies, using centrally managed services, requires explicit permission from the IT Manager; such use, whether or not authorised, may be liable to
charge.

Authorisation
In order to use the computing facilities of Alexander London College a person must first be registered. Those not automatically registered must apply to I.T. services.
Registration to use College services implies, and is conditional upon, acceptance of this Acceptable Use Policy.

The registration procedure grants authorisation to use the core I.T. facilities of the College.
Following registration, a username, password and email address will be allocated. Authorisation for other services may be requested by application to I.T. services or other providers of Information Technology based services.

Individually allocated usernames, passwords, certificates and e-mail addresses are for the exclusive use of the individual to whom they are provided. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a personal username must not be divulged to any other person, other than, in person, to known designated members of I.T. staff for the purposes of system support.

Other facilities are available for situations where staff need to share e-mail. No one may use, or attempt to use, I.T. resources allocated to another person, except when explicitly authorised by the provider of those resources, such as in those circumstances defined in this policy.

All users must always correctly identify themselves . A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice.

Privacy:
It should be noted that systems staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on any computer which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. The College fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications.
Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services.
- prevent a breach of the law, of this policy, or other College policy;
- investigate a suspected breach of the law, this policy, or other College policy; monitor standards.

Access to staff files, including electronic mail files, and/or individual I.T. usage

information will not normally be given to another member of staff unless authorised by the Head of Organisation, or Resource Manager, who will use their discretion. Procedural guidelines will be published from time to time as a separate

document. Such access will normally only be granted in the following circumstances:

- where a breach of the law or a serious breach of this or another College policy is suspected;
- when a documented and lawful request from a law enforcement agency such as the police or security services has been received; on request from the relevant Department or Section, where the managers or co-workers of the individual require access to e-mail messages or files, which are records of a

College activity, and the individual is unable e.g. through absence, to provide them. The College sees student privacy as desirable but not as an absolute right; hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

The usage of computers in College-managed laboratories, and the software installed on them, is automatically logged and are password protected; staff and students are provided with their usernames and passwords.
After a student or member of staff leaves the College, files which are left behind on any computer system owned or managed on behalf of the College, including servers and electronic mail files, will be considered to be the property of the College and is deleted once a computer system is restarted.

Behavior (The basis for effective learning and teaching)
No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the College's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer viruses and associated malware. All users of College I.T. services must ensure that any computer, for which they have responsibility, and which is attached to the College network, is adequately protected against viruses, using up to date antivirus software. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Conventional norms of behavior apply to I.T. based media, just as they would apply to more traditional media. Within the College setting this should also be taken to mean that the tradition of 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, color, nationality, ethnic origin, gender, gender identity (transsexual), marital or civil partnership status, disability, including mental health difficulties, sexual orientation, religion or belief, age, social class, pregnancy or offending background.

Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene College codes on harassment. Users of College computer systems must make themselves familiar with, and comply with, the College Code of Conduct Policy. 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.
For specific services and activities, the College may provide more detailed guidelines in addition to the policies provided in this Acceptable Use Policy.
Users of services external to the College are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. This includes social networking sites, blog and wiki services, bookmarking services and any other externally hosted services.
The use of Alexander London College credentials to gain unauthorised access to the facilities of any other organisation is strictly prohibited.

Definition of Acceptable and Unacceptable Use
Unacceptable use of College computers and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching that is permitted under UK & international law and prevent duty; propagation will normally be considered to be a much more serious offence;
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights, including use internal to the College;
- causing annoyance, inconvenience or needless anxiety to others;
- defamation (genuine scholarly criticism is permitted);
- unsolicited advertising, often referred to as "spamming";
- sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address;
- attempts to break into or damage computer systems. or data held thereon;
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software;
- attempts to access, or actions intended to facilitate access, to computers for which the individual is not authorised;
- using the College network for unauthenticated access;
- excessive I.T. use during working hours that significantly interferes with a staff member's work, or that of other staff or students;
- the retention or propagation of material/ or websites whose purpose is to promote terrorism, or which are directly linked to a proscribed terrorist organisation, except in the course of recognised research or teaching that is permitted under UK and international law.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with I.T. Services):

- the downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or permission from the copyright holder;

- the use of peer-to-peer software and related applications to illegally download and/or share music, video, film, or other material, in contravention of copyright law;
- the publication on external websites of unauthorised recordings e.g. of lectures;
- the distribution or storage by any means of pirated software;
- connecting an unauthorised device to the College network i.e. one that has not been
- configured to comply with this policy and any other relevant regulations and guidelines relating to security and acceptable use;
- circumvention of Network Access Control;
- monitoring or interception of network traffic, without permission;
- probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- associating any device to network Access Points, including wireless, for which you are not authorised;
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of I.T. services or which incur financial costs;
- excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- frivolous use of College owned computer laboratories, especially where such activities interfere with others' legitimate use of I.T. services;
- opening an unsolicited e-mail attachment, especially if not work or study-related;
- the deliberate viewing and/or printing of pornographic images;
- the passing on of electronic chain mail;
- posting of defamatory comments about staff or students on social networking sites;
- the creation of web-based content, portraying official College business without express permission or responsibility; the use of College business mailing lists for non-academic purposes; the deliberate viewing or accessing of material or websites whose purpose is to promote
- terrorism or which are directly linked to a proscribed terrorist organisation.

Other uses may be unacceptable in certain circumstances. It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken. Disciplinary action may also be taken if casual or non-work related activity results in significant problems being caused to systems or services, arising for example from browsing non-work-related websites or the downloading of software containing malicious content.

Acceptable uses may include:

- personal e-mail and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others;
- advertising via electronic notice boards, intended for this purpose, or via other College approved mechanisms

However, such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.