IT Acceptable Use Policy

MLA College IT Acceptable Use Policy
Sponsor: Head of Operations
Version 3.1 (September 2024)
Next review: August 2025

MLA College is committed to helping achieve the United Nations Sustainable Development Goals.
Whilst consideration has been given to the design of this document to reduce the use of printer ink and paper, please consider the environment before printing and only do so if absolutely necessary.

1. Aim of Policy

1.1 The aim of this policy is to ensure that MLA College's IT facilities are used: safely, lawfully and equitably.

1.2 MLA 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 the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students, staff and partners of MLA College.

1.3 This Acceptable Use Policy is intended to provide a framework for such use of MLA College's I.T. resources. It applies to all computing, telecommunication, and networking facilities provided at MLA College. It should be interpreted such that it has the widest application, in particular 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.

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

2. Scope

2.1 This policy applies to anyone using MLA College IT facilities (hardware, software, data, network access, telephony, services provided by licensed third parties, online cloud services or using MLA College IT credentials) including students, staff, and third-party individuals who have been given access for specific purposes. It is the responsibility of all users of MLA College's IT facilities to read, understand and comply with this policy and any additional policies related to their activities, including other relevant information security policies.

2.2 You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may appeal to the Head of Operations.

3. Acceptable Use

3.1 MLA College IT resources are provided primarily for academic and operational purposes to support learning and teaching, research, enterprise and the other work of MLA College.

3.2 Whilst the principles of academic freedom will be fully respected, facilities must only be used responsibly, in accordance with the law and not to bring MLA College into disrepute.

3.3 MLA College IT facilities may be accessed via MLA College owned devices or via personally owned devices but this policy is applicable, regardless of the ownership of the device used. Personally owned devices whether owned by students or staff must be maintained with up to date anti-virus software (where appropriate), system patches and kept secure. Devices provided to staff by MLA College for their personal use must also be kept secure in a similar manner.

3.4 Use of the facilities for personal activities is permitted, provided that it does not infringe the law or MLA College policies, does not interfere with others' valid use and, for staff, is not done inappropriately during their working hours. However, this is a privilege that may be withdrawn by the Head of Operations, at any point, if such use is not in accordance with this policy.

3.5 Using MLA College owned or managed services for commercial work for outside bodies, that is being undertaken on a personal basis, solely for personal gain and not through MLA College channels, requires explicit permission from the Head of Operations.

3.6 MLA College e-mail addresses and associated systems must be used for all official MLA College business, in order to facilitate auditability and institutional record keeping. All staff and students of MLA College must regularly read their MLA College e-mail.

3.7 When using MLA College's IT facilities, you remain subject to all relevant laws and policies, and, when accessing services from another legal jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service. Following the requirements of this policy, and other MLA College policies and procedures applicable to your activities, should normally ensure that you comply with the law. However, if you have any concerns about whether planned actions might be regarded as unlawful please contact the Student Support Team (students) or your line manager (staff).

3.8 You must abide by the policies and terms & conditions applicable to any other organisation whose services you access.

3.9 Further details of what constitutes acceptable and unacceptable use is provided in the subsequent sections of this policy.

4. Passwords

4.1 All default or guessable passwords for user accounts on all devices must be changed to an alternative password at the earliest opportunity.

4.2 It is recommended that you choose a password by creating a sentence and then using the first letter of each word.

> **Example** "*The first house I lived in was 61 Heavitree Road rent was £800 per month!"* would convert into TfhIliw61HRrw£8pm!
>
> **Your password must:**
> - Be at least 8 characters long
> - Contain a symbol, number and a mix of upper and lower case.
>
> **You must not**
> - Use obvious passwords such as those based on easily-discoverable information like the name of a favourite pet, family member names etc
> - Use common passwords (i.e. 'password' '123456' 'qwerty')
> - Use the same password anywhere else, at work or at home
> - Write passwords down or leave passwords in view of anyone.
> - Use password management software
> - Share passwords with other staff members

4.3 Your Office 365 and PC passwords are the most sensitive and must be memorised and not recorded anywhere.

5. Keeping Your IT Credentials Secure

5.1 You must take all reasonable precautions to safeguard your username, password and any other IT credentials issued to you. You must not allow anyone else to use your IT credentials. No-one has the authority to ask you for your password, and you must not disclose it to anyone, including the MLA College IT Service Provider.

5.2 You must not attempt to obtain or use anyone else's credentials, and you will be held responsible for all activities undertaken using your IT credentials. You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

6. Safeguarding of Information

6.1 You must take all reasonable steps to safeguard any information you have access to in accordance with the law (Data Protection Act) and MLA College's information security policies for staff and students.

6.2 You must not infringe copyright or break the terms of licences for software or other material.

6.3 You should ensure you are aware of any MLA College procedures for handling confidential information to which you have access. You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the Head of Operations (or nominee).

6.4 You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. In the event that there is a genuine academic need to carry out an activity which might be interpreted as being in breach of the law (e.g. the deliberate viewing or accessing of sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation;), MLA College must be made aware of your plans in advance and prior permission to access must be obtained from the Rector.

6.5 It is not permitted to store any personal identifiable information on removable media i.e. USB drives, USB hard drives.

7. Behaviour

7.1 The conduct of staff and students when using MLA College IT facilities should always be in line with the institution's values, including the use of online and social networking platforms. When using MLA College IT facilities you must not:

- cause needless offence, concern or annoyance to others including posting of inappropriate comments about students or members of staff (genuine scholarly criticism and debate is acceptable);
- use the IT facilities in a way that interferes with others' valid use of them;
- undertake any illegal activity including the downloading and storing of: copyright information, except under a relevant licence, or with permission from the copyright owner;
- view, store or print pornographic images or video;
- the retention or propagation of sites or media which are specifically designed 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;

- send spam (unsolicited bulk email), forge addresses, or use MLA College mailing lists other than for legitimate purposes related to MLA College activities;
- deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables;
- undertake any activity which jeopardises the security, integrity, performance or reliability of electronic devices, computer equipment, software, data and other stored information. This includes undertaking any unauthorised penetration testing or vulnerability scanning or the monitoring or interception of network traffic, without permission;
- deliberately or recklessly introduce malware or viruses;
- attempt to disrupt or circumvent IT security measures such as connecting to third party VPN services or the installation and utilisation of any application that interferes with Multi-factor Authentication (MFA) solution.
- unless otherwise approved by the Head of Operations, where remote access needs to be gained to a device connected to the MLA College network the only approved method which may be used is the MLA College's VPN platform. The use of any other remote access tools, method or system in order to gain access to a device on MLA College's network is expressly forbidden.

8. Monitoring

8.1 MLA College records and monitors the use of its IT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of:

- The effective and efficient planning and operation of the IT facilities;
- Investigation, detection and prevention of infringement of the law, this policy or other MLA College policies;
- Investigation of alleged misconduct by staff or students.
- In conjunction with MLA College's obligation to its Prevent Duty.

8.2 MLA College will comply with lawful requests for information from government and law enforcement agencies.

8.3 You must not attempt to monitor the use of the IT facilities without explicit authority to do so.

8.4 Access to workspaces, email, and/or individual IT usage information will not normally be given to another member of staff unless authorised by the Head of Operations, or nominee, who will use their discretion, normally in consultation with the Rector. Where possible and appropriate, members of the Senior Management Team will be informed, and consulted, prior to action being taken.

8.5 Where there is a requirement to access the account of another member of staff, the Head of Operations will contact MLA College's IT Service Provider with the circumstances.

8.6 If the request for access is related to a HR investigation, this should be managed wholly by an appropriate member of the Senior Management Team, as delegated by the Rector, who will work with MLA College's HR advisor and the IT Service Provider.

9. Implementation and Enforcement of this Policy

9.1 You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of the implementation of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may make a complaint under the relevant staff or student procedures.

9.2 If you believe this policy has been infringed, you should report the matter to the Head of Operations, at the earliest opportunity. Follow up action will be considered carefully. Genuinely accidental infringement will be treated with understanding but any deliberate or wilfully negligent infringement of this policy is likely to result in disciplinary action being taken under the relevant MLA Terms and Conditions or Disciplinary Policy.

9.3 Information about deliberate infringement or illegal activities may be passed to appropriate law enforcement agencies, and any other organisations whose requirements you may have breached.

9.4 MLA College reserves the right to recover from you any costs incurred as a result of your infringement.

10. Further Information

10.1 All users must comply with all relevant legislation and legal precedent, including the provisions of the following specifically related Acts of Parliament, or any re-enactment thereof:

Malicious Communications Act 1988
Computer Misuse Act 1990
Data Protection Act 1998
Regulation of Investigatory Powers Act 2000
Investigatory Powers Act 2016
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Communications Act 2003
Counter-Terrorism and Security Act (2015)
MLA College Prevent Policy