MORLEY COLLEGE LONDON

Information Technology Systems
Acceptable Use Policy

POLICY OWNER:	Chief Financial Officer
FINAL APPROVAL BY:	Policy Committee
Policy Category:	Corporate
Approved by Policy Committee:	November 2021
Approved by Governing Body:	N/A
Review Date:	November 2025

1. Introduction, Purpose and Scope of Policy:

1.1. Morley College London is committed to providing access to digital learning technology to stimulate curriculum innovation, enhance learning and address social exclusion through the acquisition of digital skills (managing information, communicating, transacting, problem-solving and creating).

1.2. This policy ensures that the Information Technology (IT) systems available from Morley College London, including audio-visual, communications, reprographic and computing resources, are used appropriately in pursuance of the College's business.

1.3. It is also intended to safeguard the College, its staff and students from information security related incidents and any consequential action, loss of income or damage.

1.4. This policy will be reviewed every four years by the Head of IT Services, or sooner if there is a notable change, for onward consideration by the Policy Committee.

2. Equality and Diversity Analysis Screening:

2.1. This policy includes safeguards regarding harassment, discrimination, and bullying, and does not discriminate based on any of the protected characteristics.

3. Applicability:

3.1. IT systems are made available to a wide range of users on a conditional basis and all users must comply with this Policy, as well as the JANET Acceptable Use Policy - https://community.jisc.ac.uk/library/acceptable-use-policy

3.2. Unless otherwise stipulated, application of this policy extends to the use of all IT systems provided by or on behalf of Morley College London, regardless of their location or the method of access.

3.3. Users accessing one or more of Morley College London's IT systems are deemed to have accepted the terms of this policy as their conditions of use.

4. Definitions:

4.1. The term "users" applies to all employees, students, governors, customers, volunteers, temporary workers, self-employed consultants, contractors, agency staff and visitors.

4.2. The term "IT Systems" refers to all audio-visual equipment, computing equipment, computer software, files, computer networks, telephone systems, mobile telephones, e-mail, internet, voicemail, and all other forms of electronic communication owned or operated by or on behalf of the College.

4.3. In this policy "data" refers to all communications and information created, sent, received, deleted, stored, or otherwise associated in any way with the College's IT systems. "Data" is not the property of any user.

4.4. In this policy, "inappropriate," "offensive," "obscene" or "pornographic" material is material that the College considers (at its absolute discretion) to be racist, sexist or otherwise discriminatory, containing nudity or images of a sexual nature or which does or could cause offence to people or, material that is illegal or defamatory.

4.5. In this policy "hacking" refers to the unauthorised use of, access to, and modification or transfer of IT systems or data, including where this leads to a disruption or denial of service; or to facilitate the commission of a crime.

5. Statutory and regulatory requirements:

5.1. Actions which are likely to contravene current legislation, may be treated as a criminal or civil offence as well as gross misconduct.

5.2. Accessing websites or material that promote terrorism or violent extremism or that seek to radicalise individuals to such causes may constitute an offence under the Counter Terrorism and Security Act 2015 and be treated as a criminal offence as well as gross misconduct.

6. Policy Objectives:

6.1. This policy ensures that all users with access to the Information Technology (IT) systems available from Morley College London, understand their responsibilities and that their use is appropriate.

6.2. It is also intended to safeguard the College, its staff and students from information security related incidents and any consequential action, loss of income or damage.

7. Policy Statement:

7.1. Morley College London's IT systems may be used to allow users to undertake activities commensurate with learning, teaching and assessment.

7.2. The College's IT systems may also be used in support of college events, academic research, college administration and for business development.

7.3. The College's IT systems may not be used:

- For personal financial interests or commercial ventures to secure personal advantage, not formally sanctioned by the College in advance
- To gain unauthorised access to IT systems, or bypass security systems
- To waste digital or physical resources including paper and consumables
- To alter or destroy the integrity of computer-based information.
- To compromise or disrupt the privacy of other users.
- To install, update or remove software unless authorised by IT Services.
- To download, store, create or view offensive or obscene material.
- For harassment, discrimination or bullying of any kind including distributing or displaying, abusive, racist, or sexist material.
- To promote terrorism or violent extremism or seek to radicalise individuals to such causes
- To make defamatory statements about a person or organisation or to post online comments that bring the College into disrepute
- For playing computer games other than those platforms authorised for student use within the College's eSports curriculum
- For on-line gambling or activities associated with cryptocurrencies
- For unsolicited commercial or advertising material, chain, or junk e-mails.
- To introduce computer viruses, trojans or other malicious software.
- For infringing copyright or intellectual property
- To stream audio visual files other than for professional or educational use
- To use the College telephone system for personal calls abroad.

- For political campaigning or fund raising, unless authorised by the College
- For any activities incompatible with an equal opportunity, multi-cultural organisation.

7.4. A formal risk assessment and justification must be provided for all users who are required to use College facilities to research terrorism or counter terrorism, which has been signed by the relevant Head of Professional Services or Curriculum.

7.5. All risk assessments must be submitted to the Designated Safeguarding Lead for review, who will consult with relevant teams including People Operations, IT Services, Estates, and the Head of Student Services, where the risk assessment relates to research involving students.

7.6. All users must have written authorisation from the Designated Safeguarding Lead before such research is commenced and for its duration.

7.7. All authorised use of college facilities to research terrorism or counter terrorism, must be time limited and communicated to the IT Service Desk in advance.

7.8. The Designated Safeguarding Lead will maintain a register of all requests to use college facilities to research terrorism or counter terrorism and report on changes to the register, to the Risk Management Committee.

7.9. All users should take reasonable steps to maintain confidentiality when using College equipment in public spaces, such as the use of privacy filters.

7.10. Limited personal use of internet and e-mail is permitted; however, it must not detract from or affect the quality or capacity of service provision.

7.11. Employees' personal use of the College's telephone system must be restricted to occasional short, urgent, or emergency calls.

7.12. All users should refrain from consuming food, liquid or smoking near IT equipment.

E-mail & Voice-mail Usage

7.13. While e-mail correspondence tends to be a more informal form of communication, UK legislation requires little formality to create a binding contract that incurs legal liabilities.

7.14. Users should therefore not enter into electronic commitments via the Internet or email unless they have explicit authority to do so.

7.15. Users should be aware that UK legislation including the laws of libel and defamation also apply to electronic documents.

7.16. When using e-mail users should follow good business etiquette and communicate in a professional manner, thinking carefully about what is said about other persons or organisations when composing e-mail messages.

7.17. Users should be mindful that e-mails may be used as an official record and therefore should not be overly familiar or informal. The use of emoticons and "text-speak" for example is not deemed appropriate when writing work e-mails.

7.18. Users should never e-mail hastily or out of anger use aggressive, abusive, or deliberately anti-social language in e-mails. The use of capitalised text in e-mail should be avoided.

7.19. Consideration should be given to alternative means of communication such as the telephone or meetings may be more appropriate when discussing complex, confidential or urgent matters.

7.20. Care must be taken when disclosing e-mail addresses to ensure it will not be misused for unsolicited e-mail, some of which may contain malicious code.

7.21. An “Out of Office” e-mail and voice message, must be used whilst users are away from the College, indicating an alternative contact and expected return date.

7.22. Users should routinely archive e-mail and voice messages when no longer needed.

Printing and Photocopying

7.23. All users should consider alternative methods to minimise costs of printing and photocopying, such as scanning documents electronically to e-mail or online storage.

7.24. The use of colour photocopying and printing should be kept to a minimum.

7.25. Energy saving features of printing and photocopying equipment must be configured to reduce the consumption of power and double-sided photocopying and printing should be adopted whenever possible, to reduce the environmental impact.

7.26. Confidential paper waste should be shredded prior to disposal and non- confidential paper waste should either be re-used or recycled.

7.27. Requests for replacement printer and photocopying consumables must be logged with the IT Service Desk and used toner recycled where possible.

7.28. All users must ensure they have permission to photocopy or scan documents and other materials to avoid infringement of copyright.

Software

7.29. No computer software of any kind may be installed on any part of the College’s IT systems, without the prior authorisation of the Head of IT Services.

7.30. All computer software must be licensed for the duration of use, as both individuals and the College can be liable in the civil and criminal courts for software theft.

7.31. Software usage must be regularly reviewed, and unlicensed software removed.

7.32. Use of computer software must adhere to the licensing terms, ensuring that the scope of licensing is sufficient for the platforms on which the software is used.

7.33. Users must work within the existing control frameworks, to use, license or install only software that has been authorised for use.

7.34. Users must seek permission from the IT Service Desk, to access software that is not on the list of the approved software.

7.35. Requests for software will be subject to a compatibility check, confirming the suitability of the platforms on which it is to be installed, to prevent the introduction of malware, incompatible or sub-standard software.

7.36. Current staff, students and governors may install software that the College provides for home use, on personal devices, subject to available licensing and terms of use.

7.37. Users must not use College IT systems to duplicate or distribute software, unless formally authorised to do so, to ensure compliance with copyright law.

7.38. All users must not attempt to reverse engineer or decompile software products unless this is explicitly permitted within the products terms of use.

Security

7.39. Authorised users are allocated a unique user account by IT Services, for which they are then responsible. Staff are also required to register for multi-factor authentication.

7.40. Users must only access the College’s IT systems using their own username and password, and not share access or divulge this information to others.

7.41. All users must ensure they register for the password reset self-service facility, change

their password regularly and use a complex password.

7.42. It is the responsibility of all users of College IT systems to comply with the College's Information and Data Protection Policy, and to ensure that information is stored securely and not disclosed to any other person unlawfully.

7.43. Users are only permitted to use their own devices when connecting to the College's wireless guest and eduroam network, providing usage is compliant with this policy.

7.44. In all other instances, the College does not permit the connection to its internal data networks, of any computing equipment that is not the College's property.

7.45. Users should ensure they log out of or shutdown their computer when they have finished using it or lock their computer when it is left unattended.

7.46. All College equipment, including that used off-site (e.g., laptops) must be physically protected to reduce the risk of unauthorised access and users are to take all reasonable steps to safeguard against loss or damage.

7.47. Users should return all College equipment made available to them at the end of any designated loan period, course, employment contract or when requested.

7.48. All computers must have up to date anti-virus software, be regularly patchedwith latest applicable security updates and have a supported operating system installed.

7.49. All e-mail and voice-mail messages originated or received on college computer and telephone systems are the property of the College.

Business Continuity

7.50. The College may from time to time authorise access to e-mail and voicemail for business continuity purposes. Requests should be made to the IT Service Desk.

7.51. Automatic back-ups of College IT systems will be administered by IT Services, with copies retained offsite and recovery tested, for the purposes of business continuity.

7.52. All staff and students are provided with data storage capacity, including home drives, shared drives, and cloud storage such as Microsoft OneDrive and SharePoint.

7.53. All users are advised to use their online storage provision and should refrain from storing data on portable media or the internal storage of personal computers.

8. Implementation of Policy:

8.1. Through the systems and processes managed by the IT Services Team and for each information system managed by others, the designated information system owner.

9. Communication and training:

9.1. The policy will be communicated through staff and student handbooks, induction, via the College's intranet, website and when connecting to the wireless network portal.

10. Monitoring and Reporting:

10.1. Use of the College's IT systems may be automatically logged to safeguard users and to permit investigation of infringements of College Policies.

10.2. Automatic scanning of e-mail and internet access is undertaken as a control mechanism to detect abuse, inappropriate language, or images, prevent viruses and malicious code from entering the network, and to ensure service continuity.

10.3. Automatic logging and filtering are deemed the least intrusive method and will be used to prevent access to websites deemed unsuitable in a work environment.

10.4. Users must contact the IT Service Desk to request a change in access to resources, including where they are blocked from accessing a website.

10.5. While this policy is non contractual, breach of any part of the policy may lead to disciplinary action and / or facilities being withdrawn.

10.6. In extreme cases where breach of this policy will be deemed to be gross misconduct, it may lead to summary dismissal.

10.7. Examples of gross misconduct include the following:

- using College IT systems to access, create or distribute offensive, obscene, or indecent material including that which is pornographic, racist, sexist, or violent or which promotes terrorism or seeks to radicalise individuals to such causes.
- deliberate or repeated introduction of computer viruses, trojans or similar malicious software.
- using College systems to threaten, harass, discriminate, or bully.
- hacking or gaining unauthorised access to computer systems.
- attempting to circumvent the College's security or monitoring systems.
- any illegal activity including the use of unlicensed software or data.
- unauthorised disclosure, alteration, transfer, or removal of data processed or stored on computer systems owned or operated by Morley College
- excessive personal or inappropriate use of College IT systems
- activities that may bring the College into disrepute.

10.8. Breach of any part of this policy may lead to disciplinary action and temporary or permanent withdrawal of access to the College's IT systems.

10.9. The College may also at its discretion withdraw or restrict access to internet sites it believes are disrupting service or being accessed excessively for personal use.

10.10. Disciplinary action will be taken in accordance with the College's student or staff disciplinary policy and procedures as appropriate.

10.11. Where the breach relates to a third party such as a contractor, the breach will be referred to the manager engaging the third party or acting as their primary contact.

10.12. All users may be liable for the costs of remedying any deliberate damage they cause to the College's IT systems.

10.13. Action taken by the College does not mean that the user may not also be liable to civil or criminal action in the courts if appropriate.

11. Related References, Policies, Procedures, Forms, and other Appendices:

11.1. Access Control Policy

11.2. Data Protection Policy

11.3. Information and Data Retention Policy

11.4. Safeguarding and Prevent Policy

11.5. Social Media Policy

11.6. Staff Disciplinary Policy

11.7. Student Disciplinary Policy