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

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.

busls l0 Tw 3.761 1 Td( )T-0.0 0 84Tc 0.002 Tw 10.5yTw 10.500.(a8.9 ()-835 (o)1 be)chs x6l1

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

6l1

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, [illegible] relevant teams in [illegible]

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 wtowtobe wto

beTimu2Æ6p2.17 (er)]TJ0 Tc 0 Tw 4.304 0 Td( )Tj-0.0
ri.(ui)2.6o(p)1(i)2(7)]TJ

be adoptg

their password regularly and use a complex password.

7.42.