MORLEY COLLEGE LONDON

Information Technology Systems
Acceptable Use Policy

POLICY OWNER: IT Services Manager
APPROVAL: 18th June 2018

NEXT REVIEW: June 2019

Equality Analysis Screening

Equality analysis is a way of considering the effects on different groups protected from discrimination by the equality act. Consider if there are any risks within this policy that will adversely affect a particular group or a variety of groups. Are there any changes that need to be made to the policy its self or additional actions that need to be made to mitigate the risks? The protected characteristics are:

- Race
- Gender
- Disability
- Age
- Sexual Orientation
- Gender reassignment
- Religion and Belief
- Maternity and Pregnancy
- Marriage and Civil Partnership

Has this Policy been identified as requiring an Equality Analysis Screening [Y/N]? N
This would need to be discussed and agreed with the Quality and Standards Manager and the Head of Human Resources. If one is required they will recommend who is involved and how this should be done.

Risks identified: None – the policy offers additional safeguards in section 4, regarding harassment, discrimination and bullying.

Evidence used (data, consultation): Consultation meeting with Head of Human Resources.

Does this policy need a further action before it can be approved?
(changes made to policy or further equality analysis needed)

No

1 INTRODUCTION AND PURPOSE

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).

Modern technology also underpins the IT strategic goals of providing an outstanding, personalised learner experience and developing efficient systems to support management across all curriculum and service functions of the College.

This policy ensures that the Information Technology (IT) systems available at Morley College London, including e-mail, the internet, telephone and computer facilities, are used appropriately in pursuance of the College's business.

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.

2 POLICY OBJECTIVES

To ensure the IT systems available at Morley College London, are used lawfully and appropriately, and to safeguard the College, its staff and students from information security related incidents.

3 SCOPE OF THE POLICY

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

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.

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

The term "IT systems" refers to all computing equipment, computer software, files generated regardless of the medium on which they are stored, computer networks, telephone systems, mobile telephones, e-mail, internet, voicemail and all other forms of electronic communication owned or operated by the College.

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.

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.

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.

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 POLICY STATEMENT

Morley College London’s IT systems may be used to allow users to undertake activities commensurate with learning, job descriptions or contracts

The College’s IT systems may also be used for events, academic research, to develop the curriculum and for professional development.

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 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 or for on-line gambling;
- For unsolicited commercial or advertising material, chain or junk e-mails;
- To introduce computer viruses, trojans or other malicious software;
- For infringing copyright;
- 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 opportunities, multi-cultural organisation.

Staff who are required to use College facilities to research terrorism or counter terrorism, must have authorisation from the Vice-Principal before such research is commenced.

Students who are required to research terrorism or counter terrorism in the course of their learning, must have authorisation from the Student Services Manager before such research is commenced.

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

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.

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

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

4.1 E-mail & Voice-mail Usage

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

Users should therefore not enter into contractual commitments via the Internet or e-mail unless they have explicit authority to do so.

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

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.

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.

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.

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.

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.

A current e-mail and where applicable, voice-mail “Out of Office” message must be used whilst employees are away from the College, indicating an alternative contact and expected return date.

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

4.2 Printing and Photocopying

Staff are provided with a unique photocopying PIN code which permits use of the black and white and colour photocopiers. This code should not be divulged to others.

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

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

Energy saving features of printer 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.

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

Requests for replacement printer and photocopying consumables must be logged with the IT Services helpdesk and used toner recycled where possible

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

4.3 Software

All computer software must be licensed as both Individuals and the College can be liable in the civil and criminal courts for software theft.

No computer software of any kind may be installed on any part of the College’s IT systems, without the written permission of IT Services.

Requests for software must be submitted to the IT Services helpdesk.

Software will only be installed if covered by a license and authorised by IT Services to ensure compliance with copyright law and to prevent the introduction of viruses or

sub-standard software which might interfere with other applications.

Users must not use College IT systems to duplicate or distribute software, unless formally authorised to do so.

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

4.4 Security and Business Continuity

Users are allocated a user name and password by IT Services, for which they are then responsible. Provision is also made for user data storage including H-drives, shared drives and cloud storage such as Microsoft OneDrive.

Users must only access the College's IT systems using their own user name and password or photocopier PIN and not divulge this information to others.

All users must ensure they change their password regularly.

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 safely and not disclosed to any other person unlawfully.

The College does not permit the connection to its network of any computing equipment that is not the College's property. Users are permitted to use their own devices when connecting to the College's wireless networks including Eduroam.

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.

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.

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

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

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

The College may from time to time authorise access to e-mail and voice-mail for business continuity purposes.

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

5 COMMUNICATION AND TRAINING

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.

6 MONITORING AND NON-COMPLIANCE

The IT systems Acceptable Use Policy will be reviewed on an annual basis by the IT Services Manager for onward consideration by the Policy Committee.

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

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.

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

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

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

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

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 & 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.

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.

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.

Disciplinary action will be taken in accordance with the College's Student Disciplinary Code or staff disciplinary procedures as appropriate.

Where the breach relates to a 3rd party such as a contractor, the breach will be referred to the employee engaging the 3rd party or acting as their primary contact.

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

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.

Actions which contravene one or more of the following, will be treated as a criminal or civil offence as well as gross misconduct:

- The Computer Misuse Act (1990)
- The Data Protection Act (1998)
- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- The Copyright, Designs and Patents Act (1988)
- Material that is likely to "deprave and corrupt" if published may constitute a criminal offence under the Obscene Publications Act
- The Telecommunications Act (1984)
- The Telecommunications (Fraud) Act 1997
- The Equality Act 2010
- Regulation of Investigatory Powers Act (2000) - (Communications Data) (Additional Functions and Amendment) Order 2006

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.