

MORLEY COLLEGE

**INFORMATION SYSTEMS
ACCEPTABLE USE POLICY
FOR LEARNERS**

Information Systems Acceptable Use Policy for Learners

1. Introduction

- a. Morley College is committed to providing learners with easy access to computing and photocopying facilities. However it needs to ensure that these facilities are used appropriately in pursuance of the College's business.
- b. This policy provides clear guidance on the use of the College's internet, photocopying and computer facilities.
- c. It is also intended to safeguard the College and its learners from information security related incidents and any consequential action, loss of income or damage.
- d. Any queries about this policy should be addressed to the IT & Technical Resources Manager.
- e. This policy will be updated as necessary.

2. Non-compliance

- a. Breach of any part of this policy may lead to disciplinary action and / or facilities being withdrawn.
- b. Disciplinary action will be taken in accordance with the College's Student Disciplinary Code
- c. Material that is likely to "deprave and corrupt" if published may constitute a criminal offence under the Obscene Publications Act and if found on the College's systems may be treated as a criminal offence as well as gross misconduct.
- d. The College may at its discretion withdraw or restrict access to internet sites it believes are disrupting service or being accessed excessively for personal use.
- e. Action taken by the College does not mean that the individual may not also be liable to civil or criminal action in the courts if appropriate.

3. Personal use

- a. Learners may have use of College internet services for personal use, however it must not interfere with course delivery or affect the quality of service provision.
- b. Learners should restrict personal use of College computer equipment to the facilities available within the Lower Library and do so in a way that is not disruptive to other Library users.

4. Acceptable Use

- a. The College's information systems are provided to allow learners to undertake activities commensurate with their studies.
- b. The College's information systems may also be used for academic research and for professional development.
- c. The College's Information Systems may not be used for:
 - *Personal financial interests or commercial ventures to secure personal advantage including profit or gain-making activities not formally sanctioned by the College;*
 - *wasting resources (e.g. people, capacity, computer equipment, consumables);*
 - *altering or destroying the integrity of computer-based information;*
 - *compromising the privacy of users;*
 - *downloading, installing or removing software without authority;*
 - *downloading, storing, creating or viewing obscene material;*
 - *making defamatory statements about a person or organisation;*
 - *playing computer games;*
 - *propagating unsolicited commercial or advertising material, chain or junk e-mails;*
 - *on-line gambling;*
 - *infringing copyright;*
 - *streaming audio and visual files not for professional use*
 - *using the College telephone system for personal calls.*
 - *political campaigning, petitions or fund raising, including activities relating to party political and single issue political campaigns or events unless agreed by the College;*
 - *any activities incompatible with the College's policies on Equality and Diversity.*

Learners who make use of the College's information systems for the following will automatically be deemed to have committed an act of gross misconduct under the College Student Disciplinary Code:

- *using College information systems to access, create or distribute , obscene or indecent material including that which is pornographic, racist, sexist or violent;*
- *deliberate or repeated introduction of computer viruses, trojans or malicious software;*
- *using College systems to threaten, harass, discriminate or bully;*
- *gaining unauthorised access to computer systems;*
- *deliberate attempt to circumvent the College's computer security & monitoring systems;*
- *any illegal activity including the use of unlicensed software or data;*
- *unauthorised disclosure, alteration or removal of data processed or stored on computer systems owned or operated by Morley College;*
- *posting online comments that brings the College into disrepute.*

- d. Learners should maintain good hygiene standards and refrain from consuming food or drink in close proximity of College computer or telephone equipment. In addition learners should not smoke in close proximity of the College's computer equipment if using it outside of the college.
- e. Learners should refrain from making any excessive noise that may disrupt others.
- f. Learners may be liable for the costs of remedying any deliberate damage they cause to the College's Information Systems.

5. E-mail

- a. 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. Learners should therefore not enter into contractual commitments via the Internet or e-mail unless they have explicit authority to do so.
- b. Learners should be aware that UK legislation including the laws of libel and defamation also apply to electronic documents.
- c. When using e-mail learners should communicate in a professional manner, thinking carefully about what is said about other persons or organisations. Learners should be mindful that e-mails may be used as an official record and therefore should not be overly familiar or informal.
- d. Learners 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.
- e. Learners should not send sexual, racially biased or other inappropriate e-mails, which would infringe the College's code of conduct.
- f. Learners should consider whether alternative means of communication such as the telephone or meeting in person, may be more appropriate when discussing complex, confidential or urgent matters.
- g. Learners should take care when disclosing their e-mail address to ensure it will not be misused for unsolicited e-mail, some of which may contain malicious code.
- h. Learners are advised to regularly delete e-mails when no longer needed.

6. Printing and Photocopying

- a. Learners are able to purchase photocopying cards from the Library, which permit use of the four black and white photocopiers in the main building.
- b. The manufacturer's guidelines should be followed at all times when using College printing and photocopying equipment.
- c. Electronic communication such as e-mail and the College VLE "Moodle" should be used in preference to paper where possible.
- d. To reduce the impact of paper usage, double-sided photocopying and printing should be adopted whenever possible and practical.
- e. Learners should ensure they have permission to photocopy or scan documents and other materials to avoid infringement of copyright.

7. Software

- a. Morley College uses computer software in all aspects of its business.
- b. The College is required by law to have a licence for every piece of software as both individuals and the College can be liable in the civil and criminal courts for software theft.
- c. No computer software of any kind may be installed on any part of the College's Information Systems without the prior permission of IT & Technical Resources.
- d. Learners should not download software from either the Internet or from e-mail attachments. Failure to observe this may breach the Copyright, Designs and Patents Act 1988.
- e. Software will only be installed if covered by a licence and authorised by IT & Technical Resources to ensure compliance with copyright law and to prevent the introduction of viruses or sub-standard software which might interfere with other applications.
- f. Learners should not use College Information systems to duplicate or distribute software either within or outside of the College, unless formally authorised to do so.
- g. Learners should not attempt to reverse engineer or decompile software products unless this is explicitly permitted within the terms of the Agreement for the use of the Product.

8. Security

- a. The College has a duty to protect its data and the IT systems that support them in order to ensure business continuity and minimise the effects of security incidents.
- b. It is the responsibility of all users of College Information Systems to comply with the College's Data Protection Policy and the Data Protection Act.
- c. Learners are allocated a user name and password upon registration with the Learning Resources Helpdesk in the Lower Library, for which they are then responsible.
- d. Learners may also be allocated a specific user account for use during IT classes.
- e. Learners should only access the College's Information Systems using their allocated user name and password and not divulge passwords to others.
- f. Learners 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.
- g. Learners should ensure they change their password regularly. Passwords expire every 90 days, must be a minimum of 8 characters and should not be repeated.
- h. All College equipment, including that used off-site (e.g. laptops) should be physically protected both to reduce the risk of unauthorised access and learners are to take all reasonable steps to safeguard against loss or damage.
- i. Learners should return all College equipment made available to them at the end of any designated loan period, or when requested.
- j. All computers should have up to date anti-virus software installed.

9. **Monitoring**

- a. The College hereby notifies learners that use of the College's Information Systems may be automatically logged to permit the investigation of infringements of College Policies.
- b. Learners are also notified that this will include automated scanning of internet access on College computer systems, undertaken as a control mechanism to
 - detect abuse, inappropriate language or images,
 - prevent viruses and malicious code from entering the network,
 - ensure service continuity.
- c. Automatic logging and filtering is deemed the least intrusive method and will be used to prevent access to websites deemed unsuitable in a working environment.
- d. Should a learner find they are blocked from accessing a website they require for their studies, they should contact the Learning Resources helpdesk.
- e. All e-mail and voice-mail messages originated or received on College computer and telephone systems are the property of the College. Learners however may prefer to use an internet e-mail account for personal e-mails (see section 4 – Personal Use).
- f. An automatic back up of College Information Systems including e-mail and Internet access will be administered by IT & Technical Resources and held offsite by a third-party storage provider for the purposes of business continuity.
- g. The College hereby notifies learners that the College premises are monitored by CCTV for security reasons.