

*ICT Acceptable Usage Policy*

March 2009

Version 2



## Document Control

---

### Changes History

| Version | Date       | Amended By      | Recipients                     | Purpose                  |
|---------|------------|-----------------|--------------------------------|--------------------------|
| 1       | 14/12/2008 | Raghu Vydyanath | Information Policies Committee |                          |
| 2       | 02/03/2009 | Raghu Vydyanath |                                | Added various legal acts |

### Related Documents

| Document   | Author | Version | Date |
|--|--------|---------|------|
| <u>JANET Acceptable Use Policy</u>                                     |        |         |      |
| <u>JANET Security Policy</u>   |        |         |      |
| <u>Combined Higher Education Software Team (CHEST) Code of Conduct</u> |        |         |      |

### Authorisation

| Role                           | Name | Signed | Date |
|--------------------------------|------|--------|------|
| Information Policies Committee |      |        |      |

### Distribution

| Name | Organisation |
|------|--------------|
|      |              |
|      |              |

## Contents

---

|                                      |   |
|--------------------------------------|---|
| 1. Introduction.....                 | 4 |
| 2. Acceptable Usage Policy.....      | 5 |
| 3. Appendix - Legal constraints..... | 9 |

# **1. Introduction**

---

## **1.1 Purpose**

This Acceptable Use Policy applies without exception to all users of ICT facilities of London Metropolitan University ( University ), be they staff, student, or a visitor with temporary access privileges, and whether registered as a user with London Metropolitan University or not.

## **1.2 Scope**

This policy covers users' activities while using any computing facilities owned by London Metropolitan University wherever those facilities may be located (e.g. a Laptop Computer taken home).

It covers users' activities while using any other computing facilities used on the London Metropolitan University campus, including personally owned PCs in Halls of residence.

It covers users of London Metropolitan University facilities who have connected over the internet or via dial-up from off campus to access London Metropolitan University resources.

All users will be deemed to be familiar with and bound by this AUP, copies of which are on the London Metropolitan University Website and Intranet Site, in all common workrooms, in all departmental offices, in the Students Union and in the Library.

## **1.3 Distribution**

This policy is located at <>

## **1.4 Exceptions**

There are no exceptions to this policy.

## **1.5 Change**

This policy is maintained by the Applications Management Team in Information Systems and Services. Requests to change the policy should be made to the Head of Applications Management. All changes will need to be approved by Information Policies Committee.

## **2. Acceptable Usage Policy**

---

### **2.1 Authorisation**

In order to use the ICT Facilities of the University a person must first be properly registered to use such services. Use of universities ICT facilities will be deemed to be acceptance of the terms and conditions of this policy.

It is expected that all users will adhere to the Universities password policy and guidelines, data protection policies in addition to all relevant university, regulatory and legal requirements.

### **2.2 Privacy and Monitoring**

The University recognises that individuals may conduct personal use of email and the Internet. However this must be kept to a minimum and be compliant with the various university and legislative requirements. If there is any doubt, please take the conservative approach and assume that it is not complaint to the university procedures and guidelines.

The University reserves the right to revoke such permission if, in the judgement of the University, these facilities are abused.

The University reserves the right for appropriately authorised staff to examine any data including personal data held on University systems or, when operationally necessary, for example to give access to a private account to a line manager or colleague. Certain staff within the University have been authorised to examine files, emails, data within individual accounts and network traffic, but will only do so when operationally necessary.

The University reserves the right to monitor email, telephone and any other electronically-mediated communications, whether stored or in transit, in line with the relevant regulatory and legislative rules/laws.

Reasons for such monitoring include the need to:

- Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes);
- Investigate or detect unauthorised use of the University's telecommunications systems and ensure compliance with this policy or other University policies;
- Ensure operational effectiveness of services (e.g. to detect viruses or other threats to the systems);
- Prevent a breach of the law or investigate a suspected breach of the law, the University's policies and contracts;
- Monitor standards and ensure effective quality control.

University staff that have access to personal data (as defined under the Data Protection Act 1998) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and manage this data is not compromised.

The University has the right to access the personal account after the staff member leaves for operational reasons and for the continuing delivery of services.

Users of ICT Facilities should be aware that the University conducts random monitoring of communications, regardless of whether the use is business or personal.

Monitoring may involve:

- Examining the number and frequency of emails;
- Viewing sent or received e-mails from a particular mailbox or stored on any server;
- Examining logs of ICT facility usage.
- Monitoring the amount of time spent on the Internet;
- Internet sites visited and information downloaded.

Where abuse is suspected (especially criminal activity and/or gross misconduct), the University may conduct a more detailed investigation involving further monitoring and examination of stored data (including employee-deleted data) held on servers/disks/drives or other historical/archived data.

Where disclosure of information is requested by the police (or another law enforcement authority) the request where possible will be handled by the University's Data Protection Officer or other relevant person.

### **2.3 Definitions of Unacceptable & Acceptable Usage**

Unacceptable use of university computers and network resources may be summarised as:

1. The following general behaviour in ICT studios and open-access areas
  - You must not consume food or drink in the vicinity of ICT equipment as it may damage the equipment and encourages vermin.
  - Excessive noise (talking, loud music) that may interfere with other users is prohibited.
  - All mobile phones must be switched off before entering an ICT area as they can interfere with other users.
  - Unreasonable behaviour (for example using facilities for games, chats etc. when others cannot access a system to carry out study related work) is not acceptable.
  - Unruly or threatening behaviour between students or towards University staff is considered a serious offence.
2. Specific to use of the ICT Facilities
  - Creating, displaying or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
  - Threatening, intimidating or harassing employees/students.
  - Using obscene, profane or abusive language.

## Acceptable Usage Policy

- Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.
- Defamation (genuine scholarly criticism is permitted).
- Unsolicited advertising often referred to as "spamming".
- Sending emails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address.
- Attempts to break into or damage computer systems or data held thereon.
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software.
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised.
- Using the University network for unauthenticated access.
- Unauthorised resale of University or JANET services or information.
- Using the ICT Facilities to conduct personal commercial business or trading.

Any other conduct which may discredit or harm the University, its staff or the ICT Facilities or is intentionally unethical / illegal even if not specifically listed in this policy is deemed unacceptable. This will be decided by the relevant University authorities.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- Downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence or other valid permission from the copyright holder.
- Distribution or storage by any means of pirated software.
- Connecting an unauthorised device to the University network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy, and acceptable use.
- Circumvention of network access control.
- Monitoring or interception of network traffic, without permission.
- Probing for the security weaknesses of systems by methods such as port-scanning, without permission.
- Associating any device to network Access Points, including wireless, to which you are not authorised.
- Non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of ICT services or which incur financial costs.
- Excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action.
- Frivolous use of University owned IT studios, especially where such activities interfere with others' legitimate use of ICT services.
- Use of University business mailing lists for non-academic purposes.
- Use of CDs, DVDs, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.
- Copying of other people's web site material without the express permission of the copyright holder.
- Use of peer-to-peer and related applications within the University. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA, and Skype. The

## Acceptable Usage Policy

current list of allowed and banned applications can be found on the Security webpages.

Users must not deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material.

If you mistakenly access such material you should notify Information Systems and Services department. You should be aware that you will be held responsible for any claims brought against the University.

In the event of any use that could be regarded as giving rise to criminal proceedings the University may inform the police or other law enforcement agency.

Other uses may be unacceptable in certain circumstances. If in doubt, it is expected that users will take the conservative view and deem that is unacceptable usage of university ICT system.

## 3. Appendix - Legal constraints

---

### 3.1 Introduction

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of University computing or communications resources shall not be copied or used without permission of the University or the copyright owner.

In particular, it is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. (This can be done through reference to the Software Licence Administrator.) Software and / or information provided by the University may only be used as part of the user's duties as an employee or student of the University or for educational purposes.

The user must abide by all the licensing agreements for software entered into by the University with other parties, noting that the right to use any such software outside the University will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under a University agreement must then be removed from it, as well as any University-owned data, such as documents and spreadsheets.

When a computer ceases to be owned by the University, all data and software must be permanently removed, in accordance with the University's policies and contractual obligations. For details on disposal see the FAQ at <http://ictservicedesk.londonmet.ac.uk/sw/selfservice/>. In the case of private work and other personal use of computing facilities, the University will not accept any liability for loss, damage, injury or expense that may result.

The user must comply with all relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

1. [Copyright, Designs and Patents Act 1988](#)
2. [Malicious Communications Act 1988](#)
3. [Computer Misuse Act 1990](#)
4. [Criminal Justice and Public Order Act 1994](#)
5. [Trade Marks Act 1994](#)
6. [Data Protection Act 1998](#)
7. [Human Rights Act 1998](#)
8. [Regulation of Investigatory Powers Act 2000](#)
9. [Freedom of Information Act 2000](#)
10. [Communications Act 2003](#)

For reference, Main points of these acts are,

1. Copyright, Designs and Patents Act 1988

This Act, together with a number of Statutory Instruments that have amended and extended it, controls copyright law, making it an offence to copy all, or a substantial part,

## Acceptable Usage Policy

which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

### 2. Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

### 3. Computer Misuse Act 1990

This Act makes it an offence:

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities;
- maliciously to corrupt or erase data or programs;
- to deny access to authorised users.

### 4. Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### 5. Trade Marks Act 1994

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose himself or herself to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

### 6. Data Protection Act 1998

The University has a Data Protection Policy <http://www.londonmet.ac.uk/staff/data-protection/policy-statement.cfm>. The policy applies to all staff and students of the

## Acceptable Usage Policy

University. Any breach of the Data Protection Act 1998 or the University Data Protection Policy is considered to be an offence and in that event, disciplinary procedures will apply.

### 7. Human Rights Act 1998

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the context of the University, important human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education

These rights are not absolute. The University, together with all users of its ICT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

### 8. Regulation of Investigatory Powers Act 2000

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications to is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The University reserves the right to monitor e-mail, telephone, and any other communications in line with its rights under this act.

### 9. Freedom of Information Act 2000

The Act, intended to increase openness and transparency, obliges public bodies, including Higher Education Institutions, to disclose a wide range of information, both proactively and in response to requests from the public.

There is an obligation to disclose any recorded information held by the University which is properly requested unless this falls within very limited exemptions and circumstances.

## Acceptable Usage Policy

The types of information that may be have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore all staff have a responsibility to know what information they hold and where and how to locate it.

### 10. Communications Act 2003

This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.