ICT Acceptable Use Policy

Author: Mark Barrow

Version: 2.0

Date: 25 September 2019

+44 (0)20 7133 4511

m.barrow@londonmet.ac.uk

**Document Control**

**Changes History**

| Version | Date | Amended By | Recipients | Purpose |
| --- | --- | --- | --- | --- |
| 1 | 13/7/2015 | A Liddiard |  |  |
| 2.0 | 25/9/2019 | M Barrow | All | Review / Update |

**Related Documents**

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Author | Version | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Authorisation**

| Role | Name | Date |
| --- | --- | --- |
| Directory of ITS | Oliver Holmes |  |

**Distribution**

| Name | Organisation |
| --- | --- |
| Leadership Team | ITS |
| Infrastructure | ITS |
| Enterprise Applications | ITS |
| Support | ITS |
| Programme Office | ITS |
| Business Management | ITS |

Contents

[ICT Acceptable Use Policy 1](#_Toc20388165)

[1. Introduction 4](#_Toc20388166)

[1.1 Purpose 4](#_Toc20388167)

[1.2 Scope 4](#_Toc20388168)

[1.3 Distribution 4](#_Toc20388169)

[1.4 Related Policies 4](#_Toc20388170)

[2. Acceptable Use 5](#_Toc20388171)

[2.1 Authorisation 5](#_Toc20388172)

[2.2 Privacy and Monitoring 5](#_Toc20388173)

[2.3 Definitions of Unacceptable & Acceptable Usage 6](#_Toc20388174)

[3. Individuals Must Not 8](#_Toc20388175)

[4. Staff Working Off Site 9](#_Toc20388176)

[5. Staff upon Termination of Contract 9](#_Toc20388177)

[6. Access to Software 9](#_Toc20388178)

[7. Legislation and Legal Requirements 10](#_Toc20388179)

[8. Exceptions Process 13](#_Toc20388180)

[9. Changes and Disputes 14](#_Toc20388181)

[5.1 Changes 14](#_Toc20388182)

[5.2 Disputes 14](#_Toc20388183)

# Introduction

### 1.1 Purpose

The Acceptable Use Policy applies, without exception, to all users of the IT facilities of London Metropolitan University. Be they staff, student or visitor and whether registered as a user with the University or not.

##

### 1.2 Scope

This policy covers users’ activity while using any computing facility owned by the London Metropolitan University, whether those facilities may be located. (EG: Laptop taken home.)

This policy covers users’ activities while using any other computing facilities used on London Metropolitan University property, including any personal IT equipment.

This policy covers users of London Metropolitan University who have connected remotely or wirelessly on any campus, using any IT resource including the Internet.

All users will be deemed to be familiar with, and bound by this policy.

### 1.3 Distribution

This policy is available

##

### 1.4 Related Policies

# Acceptable Use

### Authorisation

In order to use the IT Facilities of the University a person must first be properly registered to use any service. Use of the universities IT Facilities or IT Assets will be deemed to be in acceptance 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.

### 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 compliant to the university procedures and guidelines.

The University reserves the right to revoke any authorisations and permissions, 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 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 electronic communication, whether stored or in transit, in line with relevant regulatory and legislative rules/laws.

Reasons for such monitoring to include:

* Establishing the existence of facts, such as to provide evidence of commercial transactions in cases of dispute.
* Investigate or detect unauthorised use of University’s telecommunications systems and ensure compliance with this policy or other University policies.
* Ensure operational effectiveness of services such as to detect viruses or other threats to data and 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 (defined under the Data Protection Act and the General Data Protection Act) 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 a staff member leaves for operational reasons and for the continuing delivery of services.

Users of IT 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 emails from a particular address or domain on any server.

-Examining logs of IT facility usage

-Monitoring the amount of time spent on the internet and the destination and/or content of data contained.

-Sites visited and information downloaded.

-Cloud services and their use.

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

Where disclosure of information is requested by Police or other law enforcement, the request, where possible, will be handled by the University Secretary or other authorised person. Other than in emergency situations, all requests for personal data will be subject to authority from the Director of IT and/or The University Secretary.

### Definitions of Unacceptable & Acceptable Usage

Unacceptable use of University IT equipment, services and network may be summarised as:

* The following general behaviour in IT Studios and Open-Area access.
	+ You must not consume food or drink near IT equipment, as this may damage the equipment and encourages vermin.
	+ Excessive noise, talking and loud music, that may interfere with others users is prohibited.
	+ All mobile phones must be switched off, or made silent, before entering an IT Area as they can interfere with other users.
	+ Unreasonable behaviour, such as gaming, chats or non-educational purposes, is not acceptable.
	+ Unruly or threatening behaviour between students or towards staff is considered a serious offense.
* Unacceptable - Specific to the use of IT Facilities
	+ Creating, displaying or transmitting material that is inappropriate, fraudulent, offensive or otherwise unlawful.
	+ Threatening, intimidating or harassing of staff or students.
	+ Using obscene, profane or abusive language.
	+ Intellectual Property Rights infringement, including copyright, trademark, patent, design and moral rights.
	+ Defamation (genuine scholarly criticism is permitted)
	+ Unsolicited advertising, including spamming.
	+ Sending emails that purport to come from an individual or organisation other than the person actually sending the email.
	+ 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, malware 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 unauthorised access.
	+ Unauthorised resale of University or Janet services or information.
	+ Using IT Facilities to conduct personal commercial business or trading.
	+ Connecting devices, which have not been explicitly approved/sanctioned by the IT Department to University equipment for any purpose, including printing.

Any other conduct, which may discredit or harm the University, university staff or the IT facilities or is intentionally unethical and/or 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 would normally be considered to be a breach of this policy:

* Downloading, distributing, or storage of music, video, film or other material, for which you do not hold a valid license or valid permission from the copyright holder.
* Distribution or storage by any means of pirated software.
* Connecting an unauthorised device to the university network, a device not configured to comply with this policy or any other regulations and guidelines relating to security, purchasing policy or acceptable use.
* Circumventing of network access controls
* 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 that interfere with others legitimate us of IT facilities or which incur financial costs.
* Excessive use of resources, which may lead to denial of a service to others.
* Frivolous use of University owned IT studios, especially where such activities interfere with others legitimate use of IT services.
* Use of any storage device for the purpose of copying unlicensed copyright material, software, music etc.
* Copying of other people’s web site material without the express permission of the copyright holder.
* Use of any peer-to-peer and related applications within the University.

Users must not deliberately visit, view, download, print, copy, forward or otherwise transmit any unlawful material. This would include but not be limited to:

* Publishing or distributing material or statements, which encourage or glorify terrorism.
* Disseminating terrorist publications.
* Collecting information likely to be useful in the commissioning or preparation of terrorism.
* Downloading or distributing indecent images of children.

The University reserves the right to implement filtering to block access to unlawful material, except where access is necessary as part of legitimate research, where access to unlawful material has been specifically authorised under the University’s research ethics procedures.

If you mistakenly access unlawful material, you should notify the IT Department. You should be aware that you would 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 it is unacceptable use of the university IT services.

# Individuals Must Not

* Allow anyone else to use his or her user ID/token and password on any IT System.
* Leave their user accounts logged in at an unattended and unlocked computer.
* Use someone else’s user ID/Token and password to access any IT System.
* Leave their password unprotected (e.g. Writing it down)
* Perform any unauthorised changes to IT Systems or information
* Exceed the limits of their authorisation or specific business need to interrogate the system or data.
* Connect any non-authorised device to the physical network or directly to IT Systems.
* Store data on any non-authorised equipment (e.g. USB Drives)
* Give or transfer data or software to any person or organisation outside the University without the authority of the Director of IT and/or University Secretary.

Line Managers are required to ensure that their staff are aware, and given clear instructions on the extent and limits of a member of staff’s authority with regard to IT Systems and data.

# Staff Working Off Site

It is accepted that laptops and mobile devices will be used off site. The following controls must be applied.

* Working away from the office must be in line with the University remote working policy.
* Equipment and media taken off site should never be left unattended in public places and not left in sight in a vehicle.
* Laptops must be carried as hand luggage when travelling.
* Information/Data taken off site should be encrypted.
* Mobile devices should be protected by password and any additional security.

# Staff upon Termination of Contract

All University equipment and data should be returned to the University immediately. This includes, but not confined to, Mobile Phones, Laptops, USB Drives and Memory Sticks, CDs and DVDs.

All University data or intellectual property developed or gained during the period of employment remains the property of the University and must not be retained beyond termination or reused for any other purpose.

# Access to Software

All Users:

* Any software should not be used without the express permission of the copyright holder. All use should be in line with the software licensing requirements, and comply with the owners instructions.
* No User should copy and/or remove any software without express permission and correct licensing.
* Software licensing held externally or personally, by a user, expressly provided to them under a “Free to education”, “Free to Student”, “Free to Educator” or “Free to Academic” or is provided at a discount provided as a consequence or working or attending the University, should be either re licensed to full licensing or deleted in entirety on leaving the University employment or completing their attendance for education at the University.

#  Legislation and Legal Requirements

Users must comply, at all times, with the following Acts:

* Copyright, Design and Patents Act 1988
	+ [Copyright, Design and Patents Act 1988](https://www.legislation.gov.uk/ukpga/1988/48/contents)

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, 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 and/or sound, moving images, TV broadcasts and many other media.

* Malicious Communications Act 1988
	+ [Communications Act 1988](https://www.legislation.gov.uk/ukpga/1988/27/contents)

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.

* Computer Misuse Act 1990
	+ [Computer Misuse Act 1990](https://www.legislation.gov.uk/ukpga/1990/18/contents)

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.

* Criminal Justice and Public Order Act 1994
	+ [Criminal Justice and Public Order Act 1994](https://www.legislation.gov.uk/ukpga/1994/33/contents)

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.

* Trade Marks Act 1994
	+ [Trade Marks Act 1994](https://www.legislation.gov.uk/ukpga/1994/26/contents)

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.

* Data Protection Act 1998
	+ [Data Protection Act 1998](https://www.legislation.gov.uk/ukpga/1998/29/contents)

The University has a Data Protection Policy Statement that applies to all staff and students of the 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.

* Human Rights Act 1998
	+ [Human Rights Act 1998](https://www.legislation.gov.uk/ukpga/1998/42/contents)

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.

* Regulation of Investigatory Powers Act 2000
	+ [Regulation of Investigatory Powers Act 2000](https://www.legislation.gov.uk/ukpga/2000/23/contents)

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 or to 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.

* Freedom of Information Act 2000
	+ [Freedom of Information Act 2000](https://www.legislation.gov.uk/ukpga/2000/36/contents)

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.

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.

* Communications Act 2003
	+ [Communications Act 2003](https://www.legislation.gov.uk/ukpga/2003/21/contents)

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

* Terrorism Act 2000 and 2006
	+ [Terrorism Act 2000](https://www.legislation.gov.uk/ukpga/2000/11/contents)
	+ [Terrorism Act 2006](https://www.legislation.gov.uk/ukpga/2006/11/contents)

The Terrorism Act 2000 and the Terrorism Act 2006 create various offences relating to information, including:

 Collecting information likely to be useful in the commission or preparation of an act of terrorism.

 Publishing statements which encourage or glorify terrorism.

 Disseminating terrorist publications.

The offences are subject to certain exemptions intended to allow legitimate use. Any use of material falling under the Terrorism Acts for legitimate research purposes must first be approved under the University’s research ethics procedures. Legal advice may be required.

The Counter-Terrorism and Security Act 2015 places a duty on universities to have due regard to statutory guidance relating to the need to prevent individuals from being drawn into terrorism (the ‘Prevent Guidance’). The Prevent Guidance requires universities to have appropriate IT policies in place; to consider the use of web filtering to restrict access to harmful material; and to have policies for access to sensitive or extremism-related material for legitimate research purposes.

* Protection of Children Act 1978 and the Criminal Justice Act 1988
	+ [Protection of Children Act 1978](https://www.legislation.gov.uk/ukpga/1978/37/contents)
	+ [Criminal Justice Act 1988](https://www.legislation.gov.uk/ukpga/1988/33/contents)

These Acts penalize the possession of indecent photographs of children and the taking, making, showing, distribution, possessing with a view to distributing, and publishing any advertisement of indecent photographs of children. Downloading or printing indecent images of children from the internet is included.

Any use of material falling under this legislation for legitimate research purposes must first be approved under the University’s research ethics procedures. Legal advice may be required.

* General Data Protection Regulation 2018
	+ [General Data Protection Regulation 2018](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/)

The GDPR sets down enforceable guidelines to:

* Lawfulness, fairness and transparency
	+ Including consent, contract and obligation.
* Purpose Limitation
* Data Minimisation / Controls and accountability.
* Data Accuracy
* Data Storage Limitations
* Integrity and confidentiality. Security
* Overall Accountability and Individual Rights
	+ Right to:
		- Be informed of data (and content)
		- Access to all data
		- Rectification (data errors)
		- Erasure of all non-legal data
		- Restrict processing
		- Data portability
		- Object (Data purpose)
		- Any automated decision processes including, but not limited to, profiling.

# Exceptions Process

There are no exceptions to this policy

# Changes and Disputes

### 5.1 Changes

This policy is maintained by ITS Infrastructure department. Requests to change the policy should be made to the Director of ITS

Changes to this policy will only be accepted after submission to the Change Advisory Board.

### 5.2 Disputes

Any dispute concerning this policy should be made in writing to the Director of ITS.