Policy

University of East London

IT Services

Acceptable Use Guidance

1 Introduction

This guidance compliments the University of East London's Acceptable Use Policy. It puts into perspective specific situations that will help you provide a comprehensive understanding to complying with the universities Acceptable Use Policy. It's important to note that where a list of examples are given, they are common instances and not intended to be exhausted.

2 Purpose

The purpose of this guidance is:

- To provide a comprehensive understanding to complying with the universities Acceptable Use Policy.

3 Scope

This guidance applies to anyone using UEL IT facilities (hardware, software, data, network access, third party services, online services or *IT credentials*) provided or arranged by UEL. The terms of this guidance apply irrespective of where a user is working, whether this be on UEL premises or not

4 Guidance

A. IT Facilities

The term IT Facilities includes:

- IT Hardware that UEL provides, such as PCs, laptops, tablets, smart phones and printers
- Software that the institution provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example special deals for students on commercial application packages
- Data that UEL creates, provides, or arranges access to. This might include online journals, data sets or citation databases
- Access to the network provided or arranged by UEL this would cover, for example, network connections in halls of residence, on-campus Wi-Fi, connectivity to the internet from University PCs
- Online services arranged by the institution such as Office 365 and Google Apps, JSTOR, or any of the Jisc online resources
- IT credentials, such as the use of your UEL login, or any other token (email address, smartcard, dongle) to identify yourself when using IT facilities. For example, you may be able to use drop in facilities or Wi-Fi connectivity at other institutions using your usual username and password through the Eduroam system. While doing so, you are subject to these regulations, as well as the regulations at the institution you are visiting

B. Governance

1. Using IT has consequences in both the virtual and physical world. The use of IT facilities is governed by IT specific laws and regulations (such as these), but it is also subject to general laws and regulations that apply in the United Kingdom. The conduct of all staff, students, visitors and users of IT systems are subject to legislation relating to IT such as laws on fraud, theft and harassment.

2. An example of this would be using Janet, the IT network that connects all UK higher education and research institutions together and to the Internet.

3. When connecting to any HEI site outside UEL you will be using Janet, and subject to the Janet Acceptable Use Policy, the Janet Security Policy, and the Janet Eligibility Policy.
   The requirements of the Janet policies have been incorporated into this policy and guidance.

C. Third Party Regulations

1. If you use UEL's IT facilities to access third party services or resources you are bound by the regulations associated with that service or resource. (The association can be through something as simple as using your institutional username and password). Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it.

D. Using Chest Agreements

1. Eduserv is an organisation that has negotiated many deals for software and online resources on behalf of the UK higher education community, under the common banner of Chest agreements. These agreements have certain restrictions that may be summarised as:

   - Non-academic use is not permitted
   - Copyright must be respected
   - Privileges granted under Chest agreements must not be passed on to third parties and
   - Users must accept the User Acknowledgement of Third Party Rights.

E. Intended Use

1. The University of East London IT facilities, and the Janet network that connects institutions together and to the Internet, are funded by the tax-paying public. UEL has a duty to ensure that the facilities are being used for the purposes for which they are intended.

F. Identity

1. Users are responsible for safeguarding their own university IT credentials. It's essential that you never disclose your university IT credentials whether this is verbally or through written means with anyone including IT Services, who will never ask you to disclose your password.

2. Users must change their passwords upon first use and at regular intervals, industry practice recommends every 90 days. You should create passwords/passcodes which are difficult to guess (e.g. not "1234").

3. If you think that your password has been either been unlawfully disclosed, or someone else has been granted unauthorised access to your account, you must change your password immediately and report it to IT Services on 0208 223 2468 or through Self Service. Never enter your credentials or any sensitive information into websites which don't use HTTPS, you can see if a website uses HTTPS by looking at the sites URL, alongside a padlock which should be present, illustrating the website is secure.

4. Devices should not be left unlocked and unattended. They should be securely protected with a strong password that fulfils UEL's password criteria.

5. Shared user accounts are not permitted as this increases the security risks of account compromisation, loss of credentials and unidentifiable audit trail.

G. Infrastructure

1. The IT infrastructure comprises of equipment that make UEL's IT systems function. Some of the equipment includes; servers, PCs, printers and databases. You must not do anything to jeopardise the universities infrastructure. This includes:

    - Carrying out activities that risk damaging IT Infrastructure e.g. moving IT infrastructure without approval.
    - Reconfiguring the setup of IT Infrastructure e.g. changing network access configurations.
    - Not installing additional equipment that extends universities the universities wired or wireless network e.g. installing your own purchased Wireless Access Points (WAP's) or Wi-Fi extenders.
    - Setting up servers without explicit written authorisation from the Director of IT e.g. web servers, game servers and file sharing servers.
    - Introducing malware onto IT infrastructure, the aim of malware depends on its type however most common malware are designed to either steal or damage the system it infects e.g. through clicking on infected attachments, suspicious links or inserting infected removable devices.

2. If you see any damaged IT infrastructure, contact IT Services.

H. Software

1. Unless approved, you must not download software other than those found within the Software Centre as these applications have been tested and deployed with the latest patches and security configurations. Software installed onto UEL devices must not be removed nor adversely alter the system configuration settings. By installing software onto UEL devices you accept the user obligations where software licenses are procured by UEL.

2. Users are not allowed to purchase unauthorised software to be used for UEL business, unless written approval has been obtained from the Director of IT Services. This includes third party software which uses UEL data.

I. Information

1. Individuals must take all reasonable steps to ensure that the information they process, transmit or store is protected in line with the Data Protection Act 2018. This includes implementing access controls; to ensure only those individuals who are authorised have access to the information, have access. Encrypting sensitive data and ensuring information that is no longer required is securely deleted, in line with the universities data retention policy.

2. Information use and dissemination must be limited to the extent necessary to fulfil job responsibilities, and be in compliance with applicable policies. Before sharing Information, users must verify that they have the right to share it and that there is a legitimate business need to do so.

3. If your role is likely to involve handling sensitive information, you must make yourself familiar with UEL Data Protection Policy, alongside completing the Information Security and Data Protection training on Moodle.

4. It's discouraged to collect manually sensitive information, where possible this information should be transferred to an electronic alternative (paper documents should be scanned and securely saved).

5. When using another individual or organisations material (images, text, music, software), you have the responsibility of ensuring that you abide by the Copyright law. You should obtain permission when wanting to make use of someone else's copyright protected work and where necessary ensure references are used correctly.

6. Where information has been produced in the course of employment by UEL, and the person who created or manages it is unavailable (e.g. long term sick leave), the responsible line manager may give permission for it to be retrieved for work purposes. In doing so, care must be taken not to retrieve any private information in the account or to compromise the security of the account concerned.

7. The creation of external websites or microsites are not allowed without written approval from the Director of IT, users who need share documents, project information or files can do so through the universities Office 365 platform e.g. SharePoint, OneDrive. Academic course content can be distributed primarily through UEL's Virtual Learning Environment (VLE), more information on this can be obtained by contacting CELT.

J. Removable Media and Mobile Devices

1. Sensitive information should not be stored on removable media (USB's, CD's, External hard drives), unless encrypted. It's the responsibility of the individual performing the encryption to ensure that the keys are secure.

2. UEL issued or personal mobile device that process or store UEL data must be enrolled into the universities Mobile Device Management (MDM) system. Enrolling into the MDM system will only allow IT Services to view who the owner is, Device Name, Serial Number, Manufacturer, Model, OS and Company apps. Whilst MDM is running on the device, you should not try to circumvent or compromise Microsoft Intune's technical policies.

3. Further advice on the use and securing of removable media and mobile devices is available on the IT intranet Information Security pages.

K. Remote Working

1. Individuals who access University information offsite should ensure that they use a secure connection. A secure connection is ensuring that traffic passing over the network is encrypted. You must also be careful to avoid working in public locations where your screen can be seen and you should ensure that you do not leave information, whether it's electronic or physical (letters, reports, printouts) unattended. If a device containing university information is lost or stolen, you must contact IT Services and where possible initiate the devices remote wipe feature.

2. The university approved method for storing information in the cloud is through the use of Microsoft OneDrive, using your UEL IT account. You should not store UEL data on personal cloud services such as Dropbox, Google Drive and iCloud. When using OneDrive users are responsible for ensuring that the data in

which they upload is secure. This includes reviewing access controls, to only ensure that authorised users have access to the data.

L. Behaviour

1. Your conduct when using IT should be no different to how you would behave under other circumstances. Abusive, inconsiderate, rude or discriminatory behaviour is unacceptable.

2. Using UEL IT equipment to cause unwarranted offense or distress is not allowed and UEL has a zero tolerance on individuals carrying out any malicious activities using UEL IT equipment. Malicious activities can include hacking, distribution of SPAM, carrying out unauthorised security testing including running packet sniffing tools and scanners.
   Activities which may fall under this category for the purposes of either research or as part of a student's study, must gain prior authorisation from the Director of IT.

M. Monitoring: Institutional Monitoring

1. In order to protect the security of the information relating to UEL and its users, IT Services monitors and logs the use of its IT facilities in line with the relevant legislation for the purposes of:

   - Ensuring that it operates in a manner that is intended to safeguard the community and protect data and sensitive information.
   - Detecting, investigating or preventing misuse of the facilities or breaches of the Universities regulations
   - Monitoring the effective function of the facilities.
   - Investigation of any alleged misconduct.
   - Complying with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime and ensuring national security.
   - To ensure UEL meets its statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people drawn into terrorism.

N. Monitoring: Unauthorised Monitoring

1. You must not attempt to monitor the use of an individual or IT facilities without explicit permission from the Director of IT. This would include:

   - Monitoring network traffic;
   - Network and/or device discovery;
   - Wi-Fi traffic capture;
   - Installation of key-logging or screen grabbing software that may affect users other than yourself;
   - Attempting to access system logs, servers or network equipment;

O. Leavers

1. Unless UEL issued devices are returned to IT Services, erase Company data and access configurations prior to departing UEL, transferring ownership of the device or disposing of the device.

P. Infringement: Disciplinary Process

1. Any breach of IT policies will be subject to UEL's Staff Disciplinary Procedures for staff and Student Disciplinary Regulations for students.

2. Disciplinary could have a bearing on your future studies or employment with UEL and beyond. If in the disciplinary process, you are found to have breached a regulation sanctions may be imposed e.g. restricting access to IT facilities, removal of services, and withdrawal of offending material and recovery of any costs that have been incurred by UEL as a result of the breach of regulation.

Q. Reporting to Other Authorities

1. If UEL believe that unlawful activity has taken place, it will refer the matter to the police or other appropriate law enforcement agency in line with the Data Protection Act 2018.

5 Other Relevant Policies

a) University of East London: Acceptable Use Policy
b) University of East London: Access Management Policy
c) University of East London: Data Classification and Handling Policy
d) University of East London: Data Classification and Handling Guidance
e) University of East London: Data Protection Policy
f) University of East London: Data Storage and Retention Policy
g) University of East London: Cloud Services Policy
h) University of East London: Social Media Policy
i) University of East London: Information Security Policy
j) JANET: Acceptable Use Policy
k) JANET: Security Policy

6 Reporting

Any actual or suspected breach of the Acceptable Use Policy should be reported to IT Services immediately upon discovery. Any device in breach of this policy can be brought to IT Services who will rebuild the device to ensure compliance with the policy.

7 Failure to Comply

Failure to comply with the Acceptable Use Policy, or its subsidiary regulations, may result in withdrawal of access to University ICT Systems and may result in disciplinary action.