IT Services Policy

University of East London

Acceptable Use Policy

Table of Contents

1 Introduction

As a user of the IT systems of the University of East London (UEL) you are entitled to use its computing services. That entitlement places responsibilities on you as a user which are outlined below.

If you misuse University computing facilities in a way that constitutes a breach or disregard of the policy, this may result in disciplinary action being taken against you and may be in breach of other University Policies or Procedures. Ignorance of this policy (or those that it directs you to), and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

2 Purpose

The purpose of this policy is:

- To explicitly outline the principles for acceptable use of the University's IT facilities and services in line with any legal, regulatory and contractual requirements associated with the use of UEL facilities.

3 Scope

This policy 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 policy apply irrespective of where a user is working, whether this be on UEL premises or not.

There is specific advice on handling Payment Card data. This is covered in the Payment Card Data Protection Policy and is not specifically covered in this Acceptable Use Policy. However, those handling card payments for UEL need to follow the guidance in this policy.

4 Policy Statement

A. Intended Use

1. The University has a statutory duty under the Counter Terrorism and Security Act 2015, known as the Prevent Duty, the purpose of which is to prevent people from being drawn into terrorism. Terrorism is defined in UK law as the use or threat of action designed to influence the government or to intimidate the public or a section of the public, and the use or threat is made for the purpose of advancing a political, religious, racial, or ideological cause. UEL IT services are NOT to be used in the promotion of terrorism.
2. University IT facilities are provided primarily for academic and business operations in order to support learning and teaching, research, enterprise, businesses needs and to support a course of study for students.
3. Use of these facilities for personal activities is permitted (provided that it does not infringe any of the policy and does not interfere with your job performance or others' valid use) however personal use should be restricted during working hours and is a privilege that may be withdrawn at any time. Personal use is defined as activity that is considered non UEL related or carried out solely as part of a household activity. Users are not permitted to use UEL email for personal use activities including, but not limited to:

   - Independent business activities
   - Buying or selling goods or services
   - Promoting or marketing outside business interest

B. Identity

1. You must take all reasonable precautions to safeguard any IT credentials (for example a username and password, Multi Factor Authentication (MFA) codes, smart card, or other identity hardware) issued to you.
2. You must not allow anyone else to use your IT credentials.
3. You must not disclose your password or MFA codes to anyone, including the IT Service Desk.
4. You must not attempt to obtain or use anyone else's credentials.
5. You are accountable for all actions undertaken using your University account.
6. You must not impersonate someone else or otherwise disguise your identity when using UEL IT facilities.
7. You must not create shared accounts, whereby the same credentials for one account are distributed to multiple individuals.

C. Infrastructure

You must not do anything to jeopardise the integrity of IT infrastructure by, for example, doing any of the following without written approval from the Director, IT Services:

1. Damaging, reconfiguring or moving equipment
2. Loading software on UEL equipment other than in approved circumstances
3. Reconfiguring or connecting equipment to the network other than by approved methods
4. Setting up servers or services, including Wi-Fi, on the network
5. Setting up network monitoring tools

6. Setting up remote assistance applications to connect to devices inside of the network

7. Deliberately or recklessly introducing malware

8. Attempting to disrupt or circumvent IT security measures

9. Download malicious software

10. Seek to gain unauthorised access to restricted areas of the University's network

11. Perform security scanning, port scanning or penetration testing on UEL infrastructure or facilitating this with the use of UEL infrastructure unless a member of the IT Services IT Security Team

12. Purchase unauthorised software for UEL business

D. Information

1. You must not create, access, transmit or download extremist materials or materials which relate to terrorism or are about extremist individuals or groups using the University's IT systems or network except where you are authorised by your School to engage in academic research in this area and you are following procedures governing how you may carry out this type of research.

2. If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it whilst observing UEL's Data Protection Policy and Information Security Policy and guidance, available from UEL's website.

3. If you use a UEL issued or personal mobile device for processing UEL information, you must sign up and agree to the terms and conditions associated with UEL's Mobile Device Management system. You must ensure that the operating system on any mobile device used for UEL business is current and receives updates including security updates.

4. You must not infringe copyright or break the terms of licenses for software or other material.

5. You must adhere to user obligations where software licenses are procured by UEL. If you use any software or resources covered by a CHEST agreement, you are deemed to have accepted the Eduserv User Acknowledgment of Third-Party Rights.

6. If you are provided with Administration Rights on your UEL device, to allow software installation, you must ensure that any products you download are supported by licenses and not install unlicensed products or any product not approved by IT Services. This is to prevent dangerous or illegal products being installed.

7. You must not corrupt, alter, access or destroy another user's data without their consent, or written approval from the Director of IT.

8. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory.

9. You must not upload information or data belonging to UEL, or disclose commercially sensitive UEL data on the internet, without written approval from the Director of IT.

10. You must not create a website or microsite with the use of UEL intellectual property or branding without approval from UEB. Where such creation is approved you must ensure that any credentials for the administration of the site such as username and password are communicated to the relevant head of department.

11. You must ensure that all hard copy or physical sensitive information including personal data, business critical information and information deemed sensitive or confidential is stored in a locked area.

12. You must not leave keys for accessing drawers, filing cabinets and UEL ID cards unattended.

13. You must ensure that you do not access University sensitive or confidential information using insecure public networks (for example free Wi-Fi) where you have no choice but to use insecure public networks, you must use the UEL VPN (Cisco AnyConnect) when connecting to the UEL network.

14. You must not store sensitive or confidential University information on personal devices that are not enrolled into UEL's Mobile Device Management or Mobile Application Management programs.

15. You must not forward UEL emails to your own personal email account. It is not possible to set auto forward rules to non-UEL email accounts. [Some areas have exceptions in place for business reasons].

E. Behaviour

You are required to adhere to the highest standards of behaviour when using UEL's IT systems whether for business, educational or personal use and whether for internal or external communication:

1. You must not use UEL IT equipment to cause unwarranted offense or distress to others or perform actions that would be in breach of legislation including but not limited to the Computer Misuse Act (1990), the Data Protection Act (2018), the Regulation of Investigatory Powers Act (2000) or UEL's Data Protection Policy.

2. You must not send spam (unsolicited bulk email).

3. You must not produce material or electronic communications that brings the University into disrepute.

4. You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.

5. You must not create, download, view, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Any such activity may constitute a criminal or civil offence and will be reported accordingly.

6. You must not visit websites that contain obscene, hateful or illegal content. All browsing traffic is monitored as set out in UEL's Monitoring Policy.

7. You must abide by the regulations applicable to any other organisation whose services you access such as Janet, Eduserv and Jisc Collections. When using services via Eduroam or The Cloud wi-fi services, you are subject to both the policies of UEL and the organisations where you are accessing the services.

8. When processing personal data, you must ensure that any processing complies with the Data Protection Act (2018). More information on your responsibilities under the Data Protection Act (2018) can be found in the University Data Protection Policy.

9. You must not use and shared account for illicit purposes so as to hide your identity. Shared accounts are only created for specific business requirements with the understanding that their use will be for business need by specific individuals. Any misuse of such accounts will be considered a disciplinary offence.

10. You must not seek to hide your identity or actions by use of a non-UEL provided VPN or use of a TOR browser. Any misuse of such accounts will be considered a disciplinary offence.

F. Physical Security

1. You must protect UEL equipment and information appropriately at all times. This includes never leaving a UEL device or UEL data unattended while it is unlocked and do not put UEL devices in checked in baggage unless required by airport or similar policy.

2. You are responsible for keeping University issued devices assigned to you safe and secure. This means ensuring that you immediately notify your line manager and IT Services of any loss, stolen or damaged equipment.

3. You must not allow individual's entry into a restricted area of the University without a valid UEL ID card and such visitors must be accompanied at all times while in restricted areas. Visitors or anyone without valid ID should report to University reception to obtain the appropriate visitors pass.

G. Monitoring

1. In order to protect the business and the information of its users, UEL reserves the right to monitor and record the use of its IT facilities, including email, collaboration services and storage spaces in line with the necessary legislation and UEL's Monitoring policy which can be found on the IT Services Intranet.

2. Individual users must not attempt to monitor the use of the IT facilities using any technological or physical means.

3. You must not meaningfully subvert and/or modify data being processed by UEL IT facilities. Such action may constitute a criminal or civil offence and will be reported accordingly.

H. Leavers

On leaving UEL, staff and students' e-mail accounts will be disabled by IT Services. Prior to leaving UEL leavers must not:

1. Export UEL related email to a non UEL email address.

2. Copy, distribute or transfer any intellectual property of UEL used as part of a user's employment or study.

3. Copy, distribute or transfer any Information that could be considered Personal Data under the Data Protection Act (2018).

4. You must return all UEL devices and equipment to IT Services when leaving UEL.

5 Other Relevant Policies

a) University of East London: Account Provisioning Policy
b) University of East London: Cloud Services Policy
c) University of East London: Data Classification Policy
d) University of East London: Data Protection Policy
e) University of East London: Data Retention Policy
f) University of East London: Information Security Policy
g) University of East London: Social Media Policy
h) University of East London: Monitoring Policy
i) University of East London: Payment Card Data Protection Policy (in development)
j) JANET: Acceptable Use Policy
k) JANET: Security Policy

6 Reporting

Any actual or suspected breach of this 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 this policy, or its subsidiary regulations, may result in withdrawal of access to University ICT Systems and may result in disciplinary action.

POLICY ID:	Acceptable Use
DOC VERSION NO:	Version 2.2
DOC VERSION DATE:	April 2021
DOC AUTHOR:	Jake McMahon, Tim Moore
APPROVED BY:	Amanda Niblett
APPROVED DATE:	23 April 2021
REVIEW DATE:	April 2022