University of East London

Pioneering Futures Since 1898

Acceptable Use Policy

Contents

Need to Know Summary 3

1 Purpose and Scope of the Policy 4

1.1 Purpose 4

1.2 Scope 4

2 Policy Statement 4

2.1 General Principle 4

2.2 Personal Use 5

2.3 Unacceptable Use 5

2.4 Credentials 6

2.5 Infrastructure 7

2.6 Information 7

3 Behaviour 8

4 Email 9

5 Personal Devices 10

6 Monitoring 10

7 Reporting 10

8 Links to other Institutional Policies and Procedures 11

8.1 Internal Policies 11

8.2 Exemptions and Professional Bodies **Error! Bookmark not defined.**

University of East London

Pioneering Futures Since 1898

Policy Owner: Position and Department/School

Version	Effective From	Amendments	Equality Analysis	Stakeholders Consulted (e.g. Disability & Dyslexia Team, Policy Review Group)	Approval Date	Author	Date for Review
	Click or tap to enter a date.		Click or tap to enter a date.		Click or tap to enter a date.		Click or tap to enter a date.

Add a row each time the regulation/policy is updated (includes both minor and major updates)

This Policy is reviewed by Choose an item. and approved by Choose an item.

Need to Know Summary

This policy defines what is considered acceptable use of university IT systems, equipment, or services. It also sets out what would be considered unacceptable use. The key things you need to know are:

- IT Services and facilities are provided to staff and students to aid business, learning, or academic progression.
- You must not share your account details with anyone else.
- You are accountable for all actions undertaken using your university account.
- You must not attempt to damage, reconfigure, or move equipment.
- You must not attempt to disrupt or circumvent IT Security measures.
- You must not modify another user's data without consent from relevant individuals.
- You must not forward UEL emails to your own personal email account that do not directly relate to you as an individual.

1 Purpose and Scope of the Policy

1.1 Purpose

1.1.1 This Acceptable Use Policy sets the rules and obligations that everyone needs to be aware of when using UEL IT equipment including the use of computer hardware, software, network access. If you misuse University computing facilities in a way that constitutes a breach or disregard of this policy, you increase the risk of a cyber security incident, or a personal data breach so compliance with this policy is mandatory.

1.2 Scope

1.2.1 This policy applies to anyone that can interact with our network, data, or IT equipment. The policy applies to all employees, students, contractors, and third-party users who access UEL devices or users that use their own devices to access the UEL Network, our data or Services. This includes any information created, received, or retained, as part of university activity.

2 Policy Statement

2.1 General Principle

2.1.1

- Your UEL account is your responsibility. You must protect your credentials at all times.
- You must respect the privacy of others when collaborating and using UEL's network and infrastructure.
- You must take steps to keep UEL data safe and secure.
- You must not use UEL equipment for any illegal activity or unethical practices. Any misuse of this nature will be investigated as a disciplinary matter and may constitute a criminal offence.

2.2 Personal Use

2.2.1 Use of our network, equipment and your UEL account for personal activities is permitted if it does not infringe any UEL policy and does not interfere with your job performance or the valid use of systems or services.

2.2.2 Personal use should be restricted during working hours.

2.2.3 Personal use is defined as activity that is considered non UEL related or carried out solely as part of a personal or domestic activity.

2.2.4 While we permit limited personal use, you are not permitted to use UEL email or systems for use that relates to:

- Independent business activities.
- Buying or selling goods or services.
- Promoting or marketing outside business interest.
- Engaging in an activity that is unlawful or unethical or would likely damage the reputation of UEL.

2.2.5 While we permit limited personal use of our equipment, we reserve the right to block or prevent access to websites, services, software or applications being used on our equipment where the use would fall outside of our cyber security risk appetite.

2.3 Unacceptable Use

2.3.1 The following sets out scenarios that would be considered as unacceptable use, but this is not intended to be an exhaustive list.

2.3.2 Should the Cyber Security team become aware of any of the following we will investigate accordingly and may take action to disable your account pending a review. We may also take steps to instigate disciplinary action in some circumstances.

2.4 Credentials

2.4.1 You are accountable and responsible for all actions undertaken using your UEL account.

- You must not share or allow anyone else to use your IT credentials.
- You must not disclose your password or MFA codes to anyone, including IT Staff.
- You must not attempt to obtain or use anyone else's credentials.
- You must not impersonate someone else or otherwise disguise your identity when using UEL IT facilities.
- You must not create shared accounts, whereby the same credentials for one account are distributed to multiple individuals unless approved by IT Services.

2.5 Infrastructure

2.5.1 You must not attempt to damage, reconfigure, or move equipment including PCs without permission.

2.5.2 You are not permitted to reconfigure or connect equipment to the network other than the approved methods.

2.5.3 You must not attempt to set up servers or services, including Wi-Fi, on the network without written authorisation from the cyber security team.

2.5.4 You must not set up network monitoring tools or attempt to penetration test UEL infrastructure without permission from the IT Cyber Security team.

2.5.5 You must not set up remote assistance applications to connect to devices inside of the network.

2.5.6 You must not deliberately or recklessly introduce malware or other software designed to cause a nuisance such as Adware

2.5.7 You must not attempt to disrupt or circumvent IT Security measures.

2.5.8 You must not deliberately or recklessly consume excessive IT resources such as processing power, or bandwidth. Any consumption that degrades the availability of other services or incurs unexpected costs would be deemed excessive

2.6 Information

2.6.1 You must not, access or modify another user's personal or work-related data without their consent, or written approval from a senior manager.

2.6.2 Sharing of confidential data must only occur once authorisation has been given from the data owner. This must adhere to our Data Handling Rules, and Data Classification policy.

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

2.6.4 You must not forward UEL emails to your own personal email account that do not directly relate to you as an individual.

3 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:

- 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 UK General Data Protection Regulations, underpinned by the Data Protection Act (2018), the Regulation of Investigatory Powers Act (2000) or UEL's Data Protection Policy.

- You must not send spam (unsolicited bulk email)

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

- 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.

- You must abide by the regulations applicable to any other organization 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 organizations where you are accessing the services.

- 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

- You must not use a 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.

- 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.

- When travelling to other non-UK destinations for business operations, you must inform the IT Service Desk before you travel. Depending on the security risk of the destination, appropriate actions will be taken by IT Services to ensure that no unauthorized access to UEL data occurs during the travel.

4 Email

4.1.1 Users are provided with access to email to collaborate and communicate with other users at UEL for UEL business. Further information on the acceptable use of your email can be found in the University Email Policy.

4.1.2 You must not use your email access to attempt to phish other individuals or groups at UEL.

4.1.3 You must not use your email account to send spam to other mailboxes.

4.1.4 You must not create auto forwarding rules for UEL emails to your personal account.

5 Personal Devices

5.1.1 Personal devices used to access the UEL network must not be used to save data, or documents, locally to the device.

5.1.2 You are required to maintain compliance with the policies set out at UEL when accessing UEL services from a personal device. If UEL receive a valid request for disclosure of data such as a Subject Access Request and the data is held on a personal device, users are legally required to provide the data held on that device. Refusal to comply with a reasonable request or deliberate attempts to prevent a legitimate disclosure could constitute a criminal offence.

6 Monitoring

6.1.1 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.

6.1.2 Services and systems deployed by UEL are continuously monitored. Therefore, traffic is used to detect policy violations. If a user is found to be violating the policies, disciplinary action will be carried out.

7 Reporting

Any suspected breach of this policy should be reported to IT Services immediately upon discovery. It is the user's responsibility to report the incident to infosec@uel.ac.uk, or via our service management platform

8 Links to other Institutional Policies and Procedures

8.1 Internal Policies

This policy is underpinned by other policies designed to keep UEL secure and our data confidential. Compliance with all policies is mandatory and you should read the policies below.

- University of East London: Data Retention Policy
- University of East London: Information Security Policy
- University of East London: Data Protection Policy
- University of East London: Data Classification Policy

9 Failure to comply

Failure to comply with this policy, or its subsidiary regulations, may result in withdrawal of access to University IT Systems and may result in disciplinary action.

10 Review

This policy will be reviewed and updated by IT Services annually to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies, or contractual obligations.