Policy

University of East London

IT Services

Information Security Policy

1 Introduction

Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as the University of East London where information will relate to learning and teaching, research, administration and management. This policy is concerned with the management and security of the University's Information and the use made of this Information by its members and others who may legitimately process University information.

The Information Security Policy is the overarching document of UEL's Information Security Framework and is intended to provide an overview of Information Security best practice. This policy should be read in conjunction with the Frameworks other policies and guidance, some of which fall outside the scope of IT Services.

2 Purpose

The purpose of this policy is:

- To protect the universities IT assets and services against unauthorised access, intrusion, disruption or other damage.
- To ensure that users can maintain the confidentiality, integrity and availability of Information used within the University.
- To ensure compliance with applicable legislation and regulations.

3 Scope

This policy applies to anyone using UEL IT facilities (hardware, software, data, network access, third party services, and online services) provided or arranged by the University of East London.
It also applies to all information created, received or retained in the course of University business which must be protected according to its sensitivity, criticality and value, regardless of the media or location the data is stored or accessed from.

4 Responsibilities

Director of IT: Has ultimate accountability for implementing Information Security at UEL.

Head of Infrastructure and Security: Is responsible for ensuring that all information and information systems which are of value to UEL are adequately protected against adverse effects of Information Security breaches.

Heads of Schools and Services: Required to implement this policy and are responsible for ensuring that staff, students and other persons authorised comply with associated policies.

Individual users of UEL IT equipment/services: Are responsible for adhering to this and associated policies alongside having a duty to report any breaches of this policy, information security threats or known vulnerabilities.

5 Policy Statement

A. Awareness

1. All staff including, staff who volunteer or have a temporary contract with UEL must complete the mandatory information security awareness and data protection training available on Moodle and all users of UEL IT facilities will receive appropriate guidance in relation to information security best practices.

B. Compliance

1. This policy is in force to ensure compliance with relevant legislation and our regulatory functions.

2. UEL regards any breach of Information Security as a serious matter, which may result in disciplinary action. Additionally, where it is suspected that an offence has occurred under UK law, it may also be reported to the police or other appropriate authority who may take their own action or exercise their own powers of investigation

3. All IT services, and products used to operate those services, must be appropriately licenced.

4. All users must respect the rights of intellectual property, copyright and trademark owners.

5. UEL has a 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 being drawn into terrorism.

6. You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Such action will be considered against the Computer Misuse Act (1990) and may be considered a reportable offence.

C. User Access Control

1. All users shall have a unique identifier (user ID) for their use only; it's the user's responsibility to ensure that the User ID is not be used by anyone else and associated password must not be shared or disclosed with any other person for any reason.

2. A user's access rights are reviewed at regular intervals. If a staff member or student leaves the University IT Services will disable the users account to restrict unauthorised access.

3. Users are required to follow good security practices in the selection and use of passwords as defined in the Acceptable Use Policy.

4. Access privileges must only be authorised by the appropriate system managers, based on the minimum privileges required to fulfil an individual's duties.

D. Physical Access Controls

1. Security perimeters (barriers, card controlled entry gates and doors or manned reception desks) are used to protect areas. It is a breach of this policy to enable an unauthorised individual to enter these areas.

2. Access to areas where physical access controls are in place is logged and recorded and will be used to maintain security.

3. Access logs are reviewed on a regular basis or in the event of a security incident to identify unauthorised access.

4. All equipment and data that is located on University premises is protected from theft, loss or damage using a variety of detective and preventative means.

5. All visitors to UEL are expected to make themselves known to the relevant campus reception area and sign a visitor's log. All visitors are required to wear a visitor's pass and in restricted areas of the building should be accompanied by a member of UEL staff at all times.

6. Individuals who attempt to enter access control environments and do not have appropriate UEL ID, shall be refused access and must be reported to UEL Security immediately.

E. Network Access Controls

1. Users of UEL IT facilities should only be provided with access to the services or software that they have been specifically authorised to use as part of their role or function. Responsibility for ensuring that a user has authority to access a service should be determined by the relevant department head, who shall also ensure that user access reviews for their managed services taking place periodically.

2. Access to sensitive IT networks (such as those for Research), will be logged to enable identification of unauthorised access, whether successful or unsuccessful.

3. Security controls will also be implemented to protect local network segments and the IT resources that are attached to those segments.

4. Physical and logical access to University network points is controlled and monitored.

5. No third party (external, partners, etc.) shall receive access to UEL's network or IT equipment without explicit agreement from the Director of IT and in writing.

F. Mobile and Remote Access Control

1. Where remote access is required, this is provided via a defined access control policy to allow the minimum access necessary.

2. Security measures have been implemented to protect against the risks of using mobile computing and communication facilities including the requirement for pin protection and MDM enrolment on all UEL devices connecting to the network and accessing email.

G. Removable Media and Transmission of Data

1. IT Services have developed procedures to ensure the secure management of removable media to prevent unauthorised access. Users are expected to use recommended procedures and comply with the terms set out within the Data Storage and Retention policy which covers the secure storage and transmission of data in depth.

2. Removable media used to store sensitive data must be encrypted at all times. Guidance on how to encrypt removable media can be found on the IT intranet pages.

3. If you find a removable media device, it must not be connected to UEL infrastructure or devices. Such devices should be handed in to UEL Security for safe keeping and disposal.

4. Removal of sensitive data off site is discouraged, however under exceptional circumstances must be carried out in line with Information Security best practices and be formally authorised by a Head of Service or Department and in writing. Where the data is subject to the Data Protection Act (2018) the storage and use of the data must comply with the obligations set out in the Data Protection Policy.

H. Email Use

1. The use of IT Facilities for Email is governed by the terms set out in the UEL Acceptable Use Policy, the associated Acceptable Use Guidance and the Staff and Student handbooks.

2. All email entering or leaving the university network shall pass through the universities email filtering system which provides automated scanning of emails to detect malicious and spam emails. It will also be scanned for personal data and may be subject to Data Loss Prevention protocols as set out in UEL's Monitoring Policy.

3. Email should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken e.g. use of encryption. If you unsure of how to secure your email or if alternatives are available contact the **Service Desk.**

4. Staff and students are permitted to use email for personal use however IT Services reserve the right to access a users' UEL email account in certain circumstances, as set out in the UEL Monitoring Policy.

5. 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 for some activities including:

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

I. Internet Use

1. The use of IT Facilities for browsing the Internet is governed by the terms set out in the UEL Acceptable Use Policy, the associated Acceptable Use Guidance and the Staff and Student handbooks.

2. Users shall not use UEL Internet facilities to browse illegal or offensive material. Users are permitted to use the internet for personal use however UEL maintains a log of browsing activity for all users in order to comply with legal and regulatory requirements to permit the resolution of complaints and to investigate abuse. IT Services also have the ability to block access to websites and services that are deemed inappropriate for University use.

J. Incident Management

1. IT Services maintain an Information Security incident response plan that relies on ongoing operational monitoring and incident response procedures to be effective. If a user becomes aware of any issue that may impact up on the security of Information Security at UEL they are obliged to contact the **Service Desk** as soon as possible.

6 Other Relevant Policies

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

7 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.

8 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.

Version control							
Version No.	**Date**	**Equality analyses completed**	**Responsible officer**	**Last review**	**Next review**	**Approved by**	**Date of approval**
1.	**25 September 2018**	**Yes**	**Head of Infrastructure and Security**	**N/A**	**September 2019**	**Director of IT**	**26 September 2018**