UNIVERSITY OF WEST LONDON

Acceptable Use of Information Assets Policy

Responsibility of: IT Services
Approval Date: June 2018
Review Date: June 2020
Approved By: Vice Chancellor's Executive

1 Purpose and scope

1.1 This document applies to anyone accessing the University's Information Assets and/or using University Information Systems, with the exception of Trade Union officers and Trade Union Safety representatives acting in their official capacity in accordance with the terms of the joint agreements and statute.

1.2 The purpose of this document is to define clear rules for the use of the Information Assets provided or arranged by the University of West London.

1.3 It is also to inform Approved Users that their usage of Information Assets and Information Systems is subject to monitoring arrangements.

1.4 Use of any Information Assets that involves communication outside the boundaries of the University's Network is also governed by the JANET Acceptable Use Policy (JAUP). Trade Union Officers and Trade Union Safety representatives still remain bound by the JANET Acceptable Use Policy (AUP).

1.5 In applying this policy, the University will have regard to the need to ensure that staff have freedom within the law to question and test received wisdom and to put forward new ideas and controversial or unpopular opinions. The University will also have regard to the need to ensure that such freedom is exercised in a way which does not unduly infringe on the legitimate rights and interests of others.

2 Definitions

2.1 **Information Systems** – includes all servers and clients, portable computers, mobile phones, removable storage media, network infrastructure, system and application software, and other computer subsystems and components which are owned or used by the organisation or which are under the organisation's responsibility. The use of an Information System also includes the use of all internal or external services, such as Internet access, e-mail, etc.

2.2 **Information Assets** – in the context of this Policy, the term Information Assets is applied to Information Systems and other information/data irrespective of form, i.e. electronic information and paper documents.

2.3 **Approved Users** – refers to all members of staff and students of The University of West London and any other persons granted access to information systems.

3 Acceptable Use

3.1 The Information Assets are provided for use in furtherance of the mission of the University of West London, for example to support teaching, learning, research or in connection with your employment by the institution.

3.2 Use of these facilities for personal activities (provided that it does not infringe any of the regulations, and does not interfere with others' valid use) is permitted, but should be kept to a minimum.

3.3 Personal use is subject to the following limitations:

- it is only available for use by approved users;
- the level of use must be reasonable and not detrimental to the mission of the University;
- priority must be given to use of resources for the main purpose for which they are provided;
- personal use must not be for a commercial purpose;
- personal use must not be of a nature that competes with the University's business;

- personal use must not be connected with any use or application that conflicts with an employee's obligations to the University of West London as their employer;
- personal use must not be connected to any use or application that conflicts with the University's rules, regulations, policies or procedures, including this policy; and
- it is a privilege that may be withdrawn at any point.

3.4 Due to the insecure nature of electronic communication, the University does not accept any liability for damage or loss of whatever nature caused by the use of the email service for personal purposes. This exclusion does not apply where personal injury or death is caused by the University's negligence.

3.5 **Use of Information Systems for non-institutional commercial purposes, or for personal gain, is prohibited**.

4 Information Systems

4.1 **You must not do anything to jeopardise the integrity of the Information Systems** by, for example, doing any of the following without approval:

- Damaging, reconfiguring (e.g. disabling the anti-virus) or moving equipment (desktop PCs, printers, scanners and monitors);
- Loading software on the University equipment other than in approved circumstances;
- Reconfiguring or connecting equipment to the network other than by approved methods;
- Setting up servers or services on the network;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent any Information Security controls.

4.2 Installation of software on desktop PCs or laptops must be carried out by IT Services.

5 Information Assets

5.1 If you handle internal, restricted or confidential information, you must take all reasonable steps to safeguard it and must observe the University's Data Protection and Information Security policies and guidance, available at http://www.uwl.ac.uk/about-us/policies particularly with regard to removable storage media, mobile and privately owned devices.

5.2 You must not infringe copyright, or break the terms of licences for software or other material.

5.3 You must not attempt to access, delete, modify or disclose Information Assets belonging to other people without their permission, unless it is obvious that they intend others to do this.

5.4 Where information has been produced in the course of employment by the University, and the person who created or manages it is unavailable, it may be retrieved in accordance with the University Access to User Data policy.

6 Inappropriate material

6.1 The University of West London 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.

6.2 You must not access, create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or

extremist. The University reserves the right to block or monitor access to such material.

6.3 If such material is accessed accidentally, advice and guidance should be sought, in the case of members of staff from their line manager, and in the case of students, from their personal tutor.

6.4 The University has procedures to approve and manage valid activities involving such material for valid research purposes where legal with the appropriate ethical approval.

6.5 There is also an exemption covering authorised Information Security and IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.

7 Prohibited activities

7.1 It is **prohibited** to use information assets in a manner that unnecessarily takes up capacity, wastes staff effort or other IT resources, weakens the performance of the information system or poses a security threat. It is also **prohibited** to:

- Send unsolicited bulk or 'marketing' emails (junk) or chain emails.
- Use the University provided email address to register on websites that are not connected with teaching, learning, research or other business activities (e.g. online auction, gambling or similar websites).
- Install software on a local computer without the explicit and prior permission by the Deputy Director of IT Services.
- Access, create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, other than as set out in sections 6.4 and 6.5.
- Create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety.
- Access, create or transmit material that is either discriminatory or encourages discrimination on racial or ethnic grounds, or on grounds of gender, age, sexual orientation, marital status, disability, political or religious beliefs, other than as set out in sections 6.4 and 6.5.
- Create or transmit material with the intent to defraud.
- Create or transmit defamatory material.
- Create or transmit material such that this infringes the copyright of another person or organisation.
- Disrupt the work of other users, deny them access to services, or corrupt or destroy their data.

7.2 You should not consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. **Do not waste paper** by printing more than is needed, or by printing single-sided when double-sided would suffice. **Do not waste electricity** by leaving equipment needlessly switched on. **Use resources wisely**.

8 Taking assets off-site

8.1 Equipment, information or software, regardless of its form or storage medium, may not be taken off-site without prior written permission by the asset owner. Such permission applies when the Information Asset is taken off-site for a long period of time (more than one month) and the time limit must be clearly specified.

8.2 As long as said assets are outside the organisation, they have to be controlled by the person who was granted permission for their removal.

8.3 The use of information assets when off-campus is governed by the University mobile and remote working and mobile device policy.

9 Return of assets upon termination of contract

9.1 Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to his/her line manager or the asset owner.

10 Backup procedure

10.1 IT Services is responsible for the backup of data stored on centrally maintained systems. Such data must be backed up so that no more than 24 hours of data is at risk of loss following an incident (i.e. the Recovery Point Objective is 24 hours). Highly critical systems must be recoverable with 4 hours of an incident. Business critical systems must be recoverable within 24 hours. All other data within 3 days.

10.2 Users are responsible for backing up their own data, whether that data is stored on individual devices (PCs, laptops, mobiles) or on removable storage media or in 'the Cloud'. Users are reminded that all University data must be stored lawfully and securely. The University reserves the right to retrieve its data from any device and/or service at any time.

11 Antivirus protection

11.1 Appropriate anti-virus must be installed on each computer and have automatic updates activated.

11.2 Users must be vigilant when accessing email file attachments of accessing unknown websites.

12 Authorizations for Information Assets use

12.1 Access to the University's Information Systems will only be granted to duly authenticated users through a unique and secure user name and password combination.

12.2 Users may only access those Information Assets for which they have been explicitly authorised by the asset owner.

12.3 Users may use the Information Systems only for purposes for which they have been authorised, i.e. for which they have been granted access rights.

13 User account responsibilities

13.1 The user must take all reasonable precautions to safeguard any credentials (for example, a username and password, email address, smart card or other security token) and must not, directly or indirectly, allow another person to use his/her access rights, i.e. username, and must not attempt to obtain or use anyone else's credentials.

13.2 You must not allow anyone else to use your account. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

13.3 You must not impersonate someone else or otherwise disguise your identity when using the Information Systems provided.

13.4 The owner of the user account is its user, who is responsible for its use, and all transactions performed through this user account.

13.5 Users must follow the University Password Policy when selecting and using passwords.

14 Clear desk policy

14.1 If the authorised person is not at his/her workplace, all paper documents and data storage media containing sensitive information must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorised access.

14.2 Documents containing sensitive information must immediately be removed from printers, fax and copy machines.

14.3 Such documents and media must be stored in a secure manner.

15 Clear screen policy

15.1 If the authorised person is not at his/her workplace, all sensitive information must be removed from the screen, and access must be denied to all systems for which the person has authorisation.

15.2 In the case of short absence, the clear screen policy is implemented by logging out of all systems or locking the screen with a password. If the person is absent for a longer period of time (over 3 hours), the clear screen policy is implemented by logging out of all systems and turning off the workstation.

16 Internet Use

16.1 Access to certain Internet pages may be blocked for individual users, groups of users or all employees at the University of West London. If access to some web pages is blocked, the user may submit a written request to the University Information Security Manager for authorisation to access such pages. The user must not try to bypass such restriction autonomously.

16.2 The user is responsible for all possible consequences arising from unauthorised or inappropriate use of Internet services or content.

17 Copyright

17.1 Users must not make unauthorised copies of software owned by the organisation, except in cases permitted by law, by the owner, or by the Director of Library Services.

17.2 Users must not copy software or other original materials from other sources, and are liable for all consequences that could arise under intellectual property law.

18 Monitoring the use of information and communication systems

18.1 The University of West London monitors and logs the use of its information and communication systems for the purposes of:

- detecting, investigating or preventing misuse of the facilities or breaches of the University's regulations;
- monitoring the effective function of the facilities;
- investigation of alleged misconduct;
- complying with the obligations set out under PREVENT.

18.2 Monitoring operations will be carried out in accordance with the University Data Protection policy and with relevant legislation, including the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, and the Data Protection Act 2018.

18.3 The organisation may use specialised tools for the purpose of identifying and blocking forbidden methods of communication and filtering forbidden content.

18.4 All data which is created, stored, sent or received through the Information Systems or other University communication systems, including various applications, e-mail, Internet, fax, etc., whether it is personal or not, is considered the ownership of the University of West London. However, this clause refers to the electronic form of the data, and does not affect the author's ownership, copyright, or intellectual property rights.

18.5 Users agree that authorised persons from the University may access all such data, and that access by such persons will not be considered a violation of the users' privacy.

18.6 The content of emails and/or files stored in personal storage will only be checked in accordance to the University's Access to User Data policy.

18.7 The University will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

18.8 Any request for the disclosure of information collected as above should be made through the Data Protection Officer.

18.9 Staff who consider they have suffered unjustified detriment through the monitoring arrangements being inappropriately applied have the right to invoke the University's Grievance Policy and procedures. Likewise, students have the right to complain in accordance with the Students Complaints Procedure.

19 Unauthorised Monitoring

19.1 You must not attempt to monitor the use of information or communication systems without the explicit permission of the Associate Pro Vice-Chancellor and Chief Information Officer. This would include:

- Monitoring of 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 or servers or network equipment.

19.2 Where cyber security is itself the subject of study or research, special arrangements will have been made, and you should contact your course leader/research supervisor for more information.

20 Security Incidents

20.1 Each employee, supplier or third person who is in contact with data and/or systems of the University of West London must report any system weakness, incident or event pointing to a possible incident to the IT Service Desk.

20.2 In addition, as described in the University Data Protection Policy, all breaches of data protection should be reported immediately to the Data Protection Officer and the Information Security Manager, using the Breach Reporting Process.

21 Infringement

21.1 If you become aware of an infringement of these regulations, you must report the matter to the Information Security Manager, the Associate Pro Vice Chancellor and Chief Information Officer, or the University Secretary and Chief Compliance Officer.

21.2 The University will investigate complaints received from both internal and external sources, about any infringement of these regulations. In support of this process a technical investigation may take place, e.g. to determine the source of an offending email message.

21.3 The University may choose not to investigate anonymous or verbal complaints.

21.4 All employees are required to adhere to this policy. Any breaches may lead to disciplinary action. Serious breaches of this policy may constitute gross misconduct and lead to summary dismissal.

21.5 All students are required to adhere to this policy. Serious breaches of this policy may be a breach of the student Code of Conduct and lead to disciplinary procedures.

21.6 If the institution believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

21.7 If the institution believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

21.8 The involvement of external authorities will not prevent the University from taking appropriate action in accordance with the University's regulatory framework.