UNIVERSITY OF WESTMINSTER

Information Systems and Support – Acceptable Use Policy

1. Introduction

1.1. Purpose

The purpose of this policy is to define what constitutes acceptable use of all University information systems and infrastructure such as University-owned computer equipment, networks, services and applications. This acceptable use policy is to encourage the responsible use of facilities; to maximise the availability of resources (equipment, infrastructure and staff) for legitimate purposes; and to minimise the risk of misuse from inside or outside the University.

1.2. Scope

This policy applies to all users.

This policy covers the use of all IT services and facilities provided by the University of Westminster or by third parties on behalf of the University. These include, but are not limited to:

- In all cases, the act of registering as a user of the ISS facilities or making use of any of the IT facilities implies acceptance of conditions of use and compliance with regulations, relevant Acts of Parliament and European Union law and directives.
- All IT devices irrespective of ownership when accessing University of Westminster's services content hosted on the University of Westminster's IT facilities which is accessible via the internet by members of the public.
- Facilities and systems operated by departments for academic research, teaching and administration.

2. Condition of use of IT Facilities and Services

This policy must be adhered to at all times by all users when using/accessing University IT systems, services applications and devices. This policy also applies when users are accessing University systems, services, applications and data on non-University owned devices.

2.1. Users should be aware they must respect the copyright of all materials and software that are made available and third parties for authorised use.

2.2. Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and information which they use including software, equipment, services, documentation, and other goods including items loaned to them by the University.

2.3. Users are encouraged to use the IT facilities to further the goals and objectives of their work, study or research. All use must be for official business or research authorised by the academic supervisor or line manager of the user. Any IT activity outside this remit must be pre-approved with the Director of ISS.

2.4. Users must comply with the Computer Misuse Act of August 1990 which makes activities such as *hacking* or the deliberate introduction of viruses and other

malware a criminal offence except when part of a legitimate teaching course or legitimate and approved research activity.

2.5. Users must adhere to the provision of the Data Protection Act 2018. Accessing, deleting, amending or disclosing data or data structures of other users without their permission is a criminal offence.

2.6. Users must comply with any instructions or regulations displayed in and around IT facilities as well as instructions made available in digital format.

2.7. Users must not act in any way which puts the security of the IT services and facilities at risk.

2.8. User names and passwords must be kept safe, secure, and used only by those authorised to do so. Allowing unauthorised persons access to the University IT services or facilities by sharing passwords and user names is a criminal offence under the Misuse of Computers Act 1990 and individuals subject to disciplinary procedure.

2.9. Passwords used to connect to the University Westminster IT Systems shall conform to the requirements of the University IT Password Policy.

2.10. Where users have any control over security updates, users must apply vendor supplied security updates and critical updates as soon as practicable to systems and applications. Fixes to a vulnerability with a severity the product vendor describes as ‘critical’ or ‘high risk’, shall be applied within 14 days of release as described in the **Patching Policy**.

2.11. Users need to comply with the **IT Asset Management Policy**. This policy provides a framework for the appropriate and effective management of IT equipment (hardware and software) throughout the lifecycle of that asset.

2.12. Users are permitted to use their own personal devices to access some University systems / information, however this must be conducted within the terms of the **Bring Your Own Device Policy (BYOD).**

2.13. Users need to take mandatory security awareness training designed to help us recognise, understand and defend against the threats we all face online in our work, study and daily lives.

2.14. The definition of inappropriate use includes all unlawful activity including use of the IT facilities for possession or retention of unlawful material.

2.15. Inappropriate use includes the following activities some of which may be unlawful in the certain circumstances:

2.16. Use material or programs in a way which is unlawful, defamatory or invasive of another's privacy.

2.17. Infringe copyright works in any form including software, documents and images, audio or video recordings. Sharing of illegally held media in contravention of licensing agreements is a criminal offence and may result in a fine and/or a criminal record.

2.18. Must not load any software onto the IT facilities without written permission from ISS as defined in the **IT Administrator Policy**.

2.19. Use the IT services and facilities in such a way as to risk or to cause loss, damage or destruction of data or breaches of confidentiality of data.

2.19.1. Use the IT services and facilities in a way which infringes any patent, trademark, trade secret, copyright, moral right, confidential information or other proprietary right of any third party.

2.19.2. Publish, create, store, download, distribute or transmit material that is offensive, obscene, indecent or unlawful except in the purpose of legitimate teaching or research activities.

2.19.3. Use IT facilities in a way that brings or could bring University of Westminster into disrepute. This includes associating University of Westminster with external facilities such as Web sites that could bring University of Westminster into disrepute by association.

2.19.4. Set up equipment to provide services that they are not competent to administer, especially if such services result in security vulnerability or exposure to misuse.

2.19.5. Attempt to circumvent any firewall or software designed to protect systems against harm.

2.19.6. Jeopardise the provision of services.

2.19.7. Use of University email address to register to third party providers for personal use. For example, this may include registration of domain names for web sites for personal use.

2.19.8. Interfere with, disconnect, damage or remove equipment without approval by ISS.

2.19.9. Establish or operate wireless access points within University premises.

2.19.10. Deliberately undertake:

- any form of denial-of-service attack
- packet-sniffing or password detecting software
- port scanning
- vulnerability scanning
- execution of crypto mining software
- attempting to disguise the identity of the sender/origin of an electronic communication
- unauthorised access of the network, unsecured or unattended equipment or restricted areas of the network
- exploiting equipment compromised by malicious code
- unauthorised use of another user’s logon credentials
- unauthorised remote access of any equipment by using, for example, Terminal Services, VNC, Telnet or SSH

3. User behaviour tracking technologies

3.1. The University will ensure that it complies with the regulations and legal obligations relating to tracking user behaviour whilst using technology to access services and resources from the university.

3.2. Information collected may be used to improve security and other services for users through, for example:

3.2.1. Enabling a service to recognise your device so users don't have to give the same information several times during one task.

3.2.2. Recognising that users may already have given a username and password so users don't need to provide it for every web page requested.

3.2.3. Measuring how many people are using services, so they can be made easier to use and there's enough capacity to ensure they are fast.

3.3. When the University provides services, it wants to make them easy, useful and reliable. Where services are delivered on the internet, this sometimes involves placing small amounts of information on your device, for example, your computer or mobile phone. These include small files known as Cookies as well as other tracking technologies. They cannot be used to identify you personally but may track your behaviour on our web sites.

3.4. The University has a Website Cookies Use guidance document.

4. Condition of use of website for website owners

4.1. The University of Westminster will carry out a periodic review of web pages associated with the University and will evaluate compliance with current legislation and guidance. Web pages reported or found to be non-compliant with the legal requirements for user tracking technologies or digital accessibility regulations will be requested to review and amend their design in order to achieve compliance with the applicable law, regulations or rules.

4.2. Web page owners will be allowed a period of 30 days from receipt of the notification of non-compliance in which to take steps to modify/improve their web page design so that it is legally compliant.

4.3. Failure by the web page owner to address the issues identified in the notification will result in the University seeking reasonable remedies in order to remove the illegal web page from public access.

4.4. Should a non-compliant web page, which the University considers core to its core business activity, be hosted externally to the University network then the web page owner will be requested to resolve the compliance issues within a reasonable period of time. If the web page owner is a University colleague, then failure to comply with such a request may render the web page owner liable to internal disciplinary action by the University.

5. Mobile device management

5.1. The University uses several mobile device management (MDM) technologies for the management of University owned assets and for protecting data. This allows the University to lock/wipe devices in the event of a device being lost or stolen. The MDM service has access to asset records comprising user ID, asset tag and serial number.

5.2. ISS has the ability and reserves the right to monitor geo-location of all University owned assets to protect against nation state attacks and ensure ongoing GDPR compliance.

6. Infringement

Any infringement of the IT regulations constitutes a disciplinary offence under the applicable procedure and may be treated as such regardless of legal action and may result in access permissions being revoked.

6.1. The University reserves the right to inspect, monitor, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse as well as effective and efficient planning of the IT facilities. This includes the authorised interception and monitoring of communications as provided for by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000.

6.2. The University reserves the right to check for insecure and vulnerable systems to its network infrastructure and to block access to systems and/or services (ports) which place at risk the integrity of its network or services, or which may pose a threat to third parties.

6.3. The University reserves the right to disconnect any equipment from the University network which is deemed to be breaching policy, presenting a potential security risk or otherwise interfering with the efficient operation of the network. Equipment will not be allowed to reconnect without prior authority from ISS.

7. Procedures for dealing with misuse or suspected security violations

7.1. In the event of suspected misuse of IT facilities, ISS reserves the right to suspend user accounts and to inspect, monitor, copy or remove users' files if necessary. ISS may also disconnect network services and prevent access to the facilities without notice while investigations proceed.

7.2. The University reserves the right to refer breaches of the law to the Police. The University will comply with lawful requests for information from government and law enforcement agencies.

7.3. Breaches of this policy will result in action under the University's Academic regulations and disciplinary policies under the University's appropriate disciplinary procedures.

7.4. Users who come across any process, system or activity which they think may not be secure or look suspicious, must report it immediately to the service desk servicedesk.westminster.ac.uk No attempt should be made to investigate security vulnerabilities unless or until appropriate authority has been obtained.

8. Regulations covering the use of IT facilities and services

8.1. These Regulations cover the use of all IT facilities and services administered by the University of Westminster.

8.2. As well as these Regulations, users must abide by other policies or codes as relevant, including internal University of Westminster codes such as:

- Acceptable Use Policy
- Information Security Policy
- University IT Password Policy
- Student Code of Conduct
- Student Disciplinary Code
- Staff Disciplinary Policy
- Data Protection Policy
- Records Management Policy
- Dignity at Work and Study policy, and related documents
- Security Sensitive Research and Knowledge Exchange Activity Policy

8.3. And external codes such as:

- The acceptable use policy of the joint academic network (JANET). JANET manages network connections between Universities and Colleges and the Internet. The code is available on the JISC community website policy section.
- Public body accessibility regulations 2018.

- Access to certain University resources compels you to follow additional external codes. More information about this can be found on the University of Westminster website IT services page.

9. Related policies

9.1. This policy forms part of the information security management system (ISMS) at the University of Westminster.

9.2. The Acceptable Use Policy should be read in conjunction with all other University information management policies, which are reviewed and updated as necessary to maintain an effective Information Security Management System to meet the University's business needs and legal obligations.

10. Publishing policies

This policy is published on the University website and can be requested in a range of formats e.g. Word, PDF, plain text, alternative formats such as large print or Braille.

11. Definitions

Hacking is defined here as the unauthorized access or modification of a computer system (locally or through a network), or the use of resources that have not been allocated, with intent to access, modify or damage another's files or system files, or to deny service to legitimate users, or to obtain or alter records, or to facilitate the commission of a crime.