UNIVERSITY OF LONDON

# Acceptable Use Policy (ISP-002)

## 1 Introduction

1.1 This Acceptable Use Policy is a sub-policy of the Information Security Policy (ISP-001) and sets out the responsibilities and required behaviour of users of the University's ICT facilities.

1.2 By accessing or using the ICT facilities you agree to be bound by this policy and the overarching Information Security Policy, including all documents referred to in both.

1.3 In addition to this policy, all users of the University's ICT facilities must also comply with the JANET Acceptable Use Policy, available on the web at: https://community.ja.net/library/acceptable-use-policy.

1.4 Members of staff should refer to Appendix A for the Supplementary Acceptable Use Policy for Staff.

1.5 Residents of the University's Intercollegiate Halls should refer to the Supplementary Acceptable Use Policy in Appendix B.

## 2 Scope

2.1 For the purposes of this document, The University is defined as the central administrative and academic departments of the University of London, including the School of Advanced Study and its libraries and member Institutes, International Programmes, Senate House Library, CoSector, Student Central and the Intercollegiate Halls of Residence.

2.2 This policy applies to all staff, students, other members of the University, visitors and third parties who interact with the University's ICT facilities, collectively termed 'users' throughout this document.

2.3 ICT facilities are defined as any of the University's ICT facilities, including networks and access to the internet, email, computers, laptops, other mobile devices, and any other related software and hardware. Users using personally owned equipment attached to the University's network are also bound by this policy.

2.4 Certain staff within and outside of IT Support have a legitimate need to carry out certain IT duties as part of their job, and nothing in this policy is intended to restrict those activities. Similarly nothing in this policy is intended to restrict academic freedom, as defined in the University Statutes.

## 3 User Identification and Authentication

3.1 Members of the University will be assigned a unique account (username) for your individual use. The User Account Management Policy provides details regarding eligibility and procedures for obtaining a user account.

3.2 Users are responsible for all use of their account. You must not use another person's account, nor allow someone else to use your account.
3.3 Initial default passwords issued to any member must be changed immediately following receipt of notification of the account being set up.
3.4 Member account passwords must meet complexity requirements (at least 8 characters in length; contain at least one character from three of the following character sets: uppercase, lowercase, number and symbol; not contain a significant portion of your username and not be any one of your last ten passwords.)
3.5 You must not re-use your University account password for any other logon account or purpose.
3.6 You must not share your password with anybody. Any request for your password should be considered fraudulent and must not be granted. IT Support will never ask you for your password.
3.7 Passwords should be changed at least annually, and immediately if you suspect your account has been compromised.
3.8 You must not write down or store your password electronically in clear text (unencrypted). If you are unable to remember multiple passwords you should consider the use of a password manager.
3.9 Academic visitors from eligible institutions may access the 'eduroam' wireless internet service using their home organisation credentials. In such cases your home organisation's Acceptable Use Policy will apply in addition to this policy.
3.10 Event attendees and other academic visitors may access the Conference wireless internet service, using a daily password available at main reception.

## 4 General Conditions

4.1 You must not connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the University's wireless networks.
4.2 You must not carry out any action that may interfere with the normal working of the ICT facilities or disrupt other users' use of the ICT facilities. This includes tampering with the configuration of any University computer, network device and any associated cables or peripheral devices.
4.3 You must not attempt to circumvent or defeat security or audit controls in any way.
4.4 You must not deliberately introduce a virus, worm, Trojan horse, spyware, ransomware or other similar code nor take any action to circumvent any anti-virus or other malicious software protection installed on the ICT facilities.
4.5 You must not open attachments, follow links or reply to emails which appear to be dubious or suspicious in any way.
4.6 You should report any warning, suspicion or occurrence of a computer virus, hoax, persistent spam/phishing, denial of service or hacking attempt to ICT Support.
4.7 You must not leave your computer or portable device unattended without locking the screen or logging out.
4.8 You must ensure any screensavers are suitable for the work environment and are not likely to cause offence.
4.9 You must not install or play games on the ICT facilities.
4.10 You may use the ICT facilities for commercial activities only if you are an employee of the University or tenant organisation, and such use forms part of your duties of employment.

## 5 Legal Requirements and Prohibited Use

5.1 You must not use the ICT facilities in any way that could expose you or the University to any criminal or civil liability.

5.2 You must use the ICT facilities in accordance with the following:

5.2.1 **Computer misuse** – unauthorised access to accounts, programs and/or data (including copying, corrupting or deleting) and all forms of hacking are prohibited and may be an offence under the Computer Misuse Act 1990.

5.2.2 **Offensive material** – you must not use the ICT facilities to access, store or distribute material that is obscene, indecent or pornographic. Exceptionally, researchers who intend to access, store or distribute such material legitimately in the course of their work must seek written permission in advance from the appropriate Research Ethics Committee. In all cases, such activities must not be in breach of paragraph 5.1 above.

5.2.3 **Extremist material** - in compliance with Section 26 of the Counter-Terrorism and Security Act 2015, staff, students and visitors using University IT systems should not create, transmit, receive, view or store material with the intent to radicalise themselves or others. If a member of the University community believes they may have encountered a breach of this provision, they should contact the Office of the University Secretary immediately.

Researchers who intend to access, store or distribute such material legitimately in the course of their work must seek written permission in advance from the appropriate Research Ethics Committee. Once ethical approval has been granted, researchers should only use the University network for such activities to ensure they are flagged as a legitimate part of their research.

5.2.4 **Defamation** – you should take care to avoid content which may be defamatory. Particular care is required when sending material electronically or posting on the internet (e.g. through web pages or social media). Refer to the University's Social Media Policy for further information.

5.2.5 **Discrimination and harassment** – you must not create, distribute or access material that is unlawfully discriminatory, including on the grounds of age, sex, sexual orientation, race, disability or religion; that is likely to incite any form of violence or hatred; that is likely to cause harassment, alarm or distress; or contravenes the University's Equality Policy.

5.2.6 **Data** – all data owned, processed or held by the University, whether primary or secondary, must be accessed, stored, transmitted, processed and backed up in a manner appropriate to its security classification. Refer to the University's Data Classification Policy for further information. In particular, attention is drawn to data classified as high risk/impact which must not be transmitted or stored on removable media/portable devices in unencrypted form.

5.2.7 **Personal Data** - data on living persons must be held and processed in accordance with the Data Protection Act 1998. Persons who hold personal data are, with few exceptions, required to notify the Information Commissioner of details of their processing of data, which must in any event be in accordance with the data protection principles set out in the Act. Refer to the University's Data Protection Policy for further information.

5.2.8 **Software** – software may only be installed on the ICT facilities by authorised staff and should always be used in accordance with the terms of the relevant license agreement. Copying and distribution of licensed software is prohibited.

5.2.9 **Rights in content** – do not use third party text, images, sounds, trademarks or logos in materials such as emails, documents and web pages without the consent of the rights holder.

5.2.10 **Unsolicited and offensive email** – you must not initiate or forward email chain letters, jokes or other mass emails (spam). You must not send email that any member of the University or wider community may reasonably find offensive or likely to cause annoyance or needless anxiety, in particular any that would be in breach of sub-paragraphs 5.2.2 to 5.2.5 above.

5.2.11 **Formation of contracts** - you should note that it is possible to form contracts electronically, without any hard copy confirmation from the user. Care should be taken to obtain appropriate authority before purporting to commit the University to any contractual obligations (which may include clicking 'I agree' to an online dialogue box) and the wording 'subject to contract' should be used on emails where appropriate.

## 6 Personal Use

6.1 The ICT facilities are made available for you to use principally for the purpose of your work or studies. However, reasonable personal use of the facilities (including online banking, shopping or use of social media sites) in your normal breaks or outside working hours is acceptable if such use:

6.1.1 does not interfere with the performance of your work or studies;

6.1.2 does not incur unwarranted expense on the University;

6.1.3 does not have a negative impact on the University; and

6.1.4 is otherwise in accordance with this Acceptable Use Policy

## 7 Monitoring and Privacy

7.1 The University undertakes some routine monitoring of activity on the ICT facilities to ensure that they operate correctly and to protect against the risk of harm from viruses, malicious attack and other known threats. This does not normally involve the monitoring of individual communications or the disclosure of the contents of any user files.

7.2 The University reserves the right to monitor your use of the ICT facilities, including emails sent and received, and web pages or other online content accessed:

7.2.1 to protect the IT Facilities against viruses, hackers and other malicious attack;

7.2.2 to assist in the investigation of breaches of this and other relevant University policies;

7.2.3 to prevent or detect crime or other unauthorised use of the IT Facilities;

7.2.4 when legally required to do so, for example as part of a police investigation or by order of a court of law;

7.2.5 where such monitoring is necessary, to pursue the University's other pressing academic and business interests, for example by reviewing the emails of employees on long-term sick leave or to disclose documents under the Freedom of Information Act 2000.

7.3 In all cases, monitoring of individual content shall only be carried out if authorised by the Director of ICT, and: the Director of HR for members of staff, visitors and third parties; the Dean or Deputy Chief Executive of SAS for School of Advanced Study students; and the Chief Executive or Deputy CE of UoLIP for International Programmes students. An impact assessment must first be carried out to take into account the justification of the monitoring and the need to observe academic freedoms. Monitoring will normally continue for a maximum of three months but may be extended if justified in the light of an updated impact assessment.

7.4 Any information collected during the course of the monitoring will be held securely in accordance with the University's Data Protection Policy. You will be given the opportunity to see and explain any data collected, as part of any disciplinary or grievance procedures that may result.

## 8 Policy Awareness and Disciplinary Procedure

8.1 This policy will be provided to all new and existing staff, students and members of the University. All other users of the University's information systems will be advised of the existence of this policy, which will be made available on the University website.

8.2 All users are required to familiarise themselves with this policy and comply with its requirements.

8.3 Where an alleged breach of these conditions has occurred, all reasonable measures will be taken to investigate whether the allegation is justified and, if so, the necessary steps will be taken to prevent further abuse. This may involve the authorised inspection of a user's files or email messages as described in paragraph 7 above.

8.4 If a complaint or allegation is received, your access to the ICT facilities may be immediately suspended without notice, pending investigation. Wherever possible, users will be notified of such suspension.

8.5 Penalties for breach of this policy may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances legal action may be taken. The University may refer the user to the police where it reasonably believes a crime has been committed and will co-operate fully with any police investigations.

## 9 Version Control

| Date | Version | Purpose/Change | Author |
|---|---|---|---|
| 11/10/2016 | 0-1 | Initial draft | IT Security & Business Continuity Manager |
| 07/11/2016 | 0-2 | Consultation draft – to working group | IT Security & Business Continuity Manager |
| 02/12/2016 | 0-3 | Second consultation draft – to incorporate HoR terms and conditions | IT Security & Business Continuity Manager |
| 05/12/2016 | 0-4 | Third consultation draft – to working group | IT Security & Business Continuity Manager |
| 21/02/2017 | 1-0 | Final version – approved by the Information Technology Governance Group (ITGG) and the Joint Negotiating and Consultation Committee (JNCC) | IT Security & Business Continuity Manager |

**APPENDIX A**

## Supplementary Acceptable Use Policy for Staff

### 1 General Email

1.1 Staff must exercise extreme caution when sending emails to any destination, and automatically forwarding emails to an external destination (such as third party personal email), is strictly forbidden.
1.2 Data classified as High or Medium may not be sent or forwarded from your University email account unless that email is critical to business and appropriately encrypted.

### 2 Email on Mobile Devices

2.1 The University recognises that the majority of staff have personal smartphones and wish to access University email on these devices. This is permitted provided the following conditions are met:
2.1.1 The device has remote wipe capability
2.1.2 The device is protected by a PIN
2.1.3 The number of emails is limited to either 100 emails or the last 2 weeks
2.1.4 You delete any data classified as High risk once it has served its purpose
2.1.5 You must contact the IT Service Desk immediately if the device is lost or stolen so that they can remote wipe the device.
2.2 Any mobile device which does not have remote wipe capability is not permitted to connect to University email services.
2.3 You must ensure that mobile devices are never left unattended.
2.4 Mobile devices should be encrypted where supported.

### 3 Storage of data

3.1 Ensure that all critical data is stored either on an appropriate University server (e.g. Fileshare) or in the Office365 cloud environment (OneDrive or SharePoint) rather than on your PC/laptop's local hard drive. This ensures that the data can be backed up and removes the risk of loss due to local hard disk failure.
3.2 You are not permitted to store or transfer University data using third party file sharing sites, such as Dropbox. Large files may be shared either via Office365 or using the University's secure file transfer service, WebDrop: https://webdrop.london.ac.uk/

### 4 Remote Working and Use of Personal Equipment

4.1 The University recognises and supports the adoption of remote working, which is a key component of Smarter Working, otherwise known as Activity Based Working (ABW) but staff must be aware of the additional security measures which must be taken.
4.2 Remote working must be undertaken in accordance with the following:

4.2.1 **Public Wi-Fi** – must be used with extreme caution, only used for work purposes when absolutely essential and never for accessing data classified as high risk. Always check the authenticity of Wi-Fi hotspots and do not assume the strongest signal is a legitimate service. Always manually select networks and turn off Wi-Fi capability when not in use.

4.2.2 **Public locations** – you must be aware of your surroundings and the need to maintain confidentiality when working in public. Do not allow other people to view your screen or printed material, and do not conduct sensitive conversations that should not be overhead. Always keep mobile devices close to you and lock your screen or shut down your device when not in use.

4.2.3 **Home network** – you must ensure that you have secured your home network to best practise prior to connecting to the ICT facilities from home. Please see: https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/securing-your-home-network

4.2.4 **Accessing web based application** – to ensure that no University data is inadvertently transferred to unprotected personal computers or laptops, the University does not permit direct access from these devices to web based applications such as Office365, SITS, Agresso and Kinetics. The following list describes the supported methods staff may access these applications:

4.2.4..1 Using your University of London provided laptop or Surface, which are protected with Bitlocker encryption.

4.2.4..2 Using the Homeworking Portal from your personal computer (from June 2017)

4.2.4..3 Using VPN and Remote Desktop to your University PC.

## 5 Staff Profile Pictures

5.1 Staff are encouraged to upload a photograph of themselves on their Skype for Business account and Office 365 Staff Directory to help other staff with the identification of colleagues across the many departments of the University. Your picture must:

5.1.1 Be a quality head and shoulders photograph of true likeness.

5.1.2 Be suitable for business use (e.g. no sunglasses, comical expressions, etc.)

5.1.3 Only include you as the subject. It should not include any other persons, objects, animals, etc.

## APPENDIX B

## Supplementary Acceptable Use Policy for Residents of Intercollegiate Halls

1.1 **General** - Please be aware that by signing the Hall regulations form you are agreeing to abide by both this policy and the JANET Acceptable Use Policy. As with all Hall regulations, this agreement is personal to you. Thus, you are liable for any misuse of the internet connection provided in your accommodation and therefore subsequent misuse of the University's computer network and/or JANET connection. You are strongly advised to password protect your computer and turn it off when not in use, especially if you occupy shared accommodation.

1.2 **Misuse of the service** - Any complaints indicating misuse of the internet service are routinely investigated. Where clear evidence is provided that allows misuse to be traced to a specific room connection, we may suspend that connection without notice to prevent further misuse of the internet service. The relevant resident will then be contacted via the Halls of Residence administration team to investigate the matter further. In cases of continual misuse of the internet service the University may choose, at its discretion, to terminate connection to the internet service for the remainder of your residence contract or provide an internet service which is configured to prevent further misuse.

1.3 **Resource Usage** - The internet service is delivered on a network provided for the furtherance of your academic aims. Therefore, whilst reasonable personal use of the network is permissible, use of the network for furthering your academic aims should always take precedence. Support and provision of the internet service are conducted with this in mind. Unfortunately this also means that work of a commercial nature is not permitted and we are unable to provide support for problems arising from using the internet service for this purpose. Where clear evidence exists that a resident or member of a resident's family is using the internet service for commercial activity they will be formally requested to cease this activity. Subsequent activity of this nature will result in suspension of the internet service and referral to the Halls of Residence administration team for action to be taken under disciplinary procedures.

1.4 **Complaints of Copyright Infringement** – The University routinely investigates all complaints of copyright infringement, which are handled in the following way:

a. On the wired internet service where there is no doubt as to which connection was in use at the time, we will quarantine the relevant room internet connection. On the wireless internet service, excluding users of Eduroam, we will disable the relevant logon account. In both cases the device associated with the copyright infringement complaint will be prevented from connecting to the internet service.

b. The relevant Hall of Residence administration team will then be contacted by the IT helpdesk and provided with the copyright infringement notice from the third party and an email to be sent to either the person(s) named on the residence contract for the relevant room or to the user of the wireless account. The helpdesk will then wait for a response.

c. Once the helpdesk receives a response they will advise what is required for in order for reconnection to the internet service. Typically this will be to respond to the copyright holder, delete the infringing material and agree to the network terms & conditions. However not all copyright holders handle things in the same way so the above is a guide only.

d. Once the helpdesk are satisfied that all of the requirements for reconnection have been met, the relevant connection/account will be removed from quarantine or enabled as appropriate.

1.5 Where a further complaint of copyright infringement is traced to a resident who has already been through the above process the connection to the internet service is suspended as per step ‘a’ above. The matter is then referred to the Halls Administration teams to be taken through the Halls of Residence disciplinary process. The internet service will remain suspended until the outcome of the disciplinary has been received in writing from the Halls of Residence administration team. It should be made clear that it is not guaranteed that the suspension of the internet service will be lifted as part of the disciplinary process.

1.6 Users of eduroam for whom copyright complaints are received will have their user account details passed onto their home academic institute. The home institution then deals with the copyright infringement under their own procedures for such matters. No further action is taken by the SWAN IT helpdesk in these cases.

1.7 **Limitations of Liability** - Whilst every effort is made to prevent disruption to internet services, the University does not warrant that an internet connection will be available at all times and cannot be held liable for any loss or damage (including consequential loss) caused by disruption to JANET, the University network and servers, or abuses by another user. It is each user's responsibility to ensure that any equipment used is in proper working order and is fitted with a suitable means to connect to and use the provided internet services.

1.8 **Viruses** - It is your responsibility to maintain your computer to prevent virus infection. Should the University detect or be notified of virus activity on the internet service, the device or connection, where it can be clearly identified, will be blocked or suspended without notice. Where clear identification of either the user or the room/accommodation unit is possible, the helpdesk will send an email via the Halls of Residence administration team advising you why we have blocked/suspended the internet service. Reconnection to the internet service will be restored once the SWAN support team are satisfied that the device deemed to be infected is virus free and is in a condition that reduces the likelihood of further virus infection. Typically this is done on a trust basis the first time around with advice provided by the support team as to the best course of action and requirements for reconnection.

1.9 If a device is infected a second time, the device will need to be inspected and cleared for reconnection by a member of the SWAN support team. Typically, the support team will request that the device is submitted for inspection at Senate House, where a member of the support team will inspect your device in your presence. Where a device is found to be in a condition likely to cause further virus infection recommendations will be made as to what is required to allow re-connection. A further re-inspection will then be required to confirm the recommendations have been implemented. Whilst the support team will not hold up any inspection unduly, an inspection can only be done on a pre-arranged basis, where possible an inspection will be carried out within 5 working days of you contacting the IT support desk. It should however be noted that inspections are not regarded as high priority work and therefore there maybe times where it is not possible to arrange an inspection within these timeframes.