UNIVERSITY OF LONDON | INTERCOLLEGIATE HALLS OF RESIDENCE

Halls of Residence Internet Services Information & Conditions of Use 2016-17

Provision of Internet Services & General Information

The University is normally able to provide access to the internet from your room or accommodation unit by means of either a wired or wireless connection. In some cases both types of connectivity maybe available. Wireless (Eduroam Network) is also typically found in the reception areas and other large communal spaces and facilities within your Hall of Residence. Details of these areas can be provided by the IT helpdesk or by your Hall of Residence administration team.

To access the internet service using the wired connection, you will require a device fitted with an Ethernet card, more commonly known as a network card. A data cable is also required and is provided free of charge by the Halls of Residence. The cable can be obtained from the front desk at your Hall of Residence if there is not a cable in your room or the cable you have has broken securing tabs.

To access the internet service using the wireless service you will require a device that is fitted with a wireless card and that is able to use the security and encryption settings of WPA2/AES. Most modern devices will be able to do this, early or so called legacy devices may not be able to meet this minimum and these would require you to upgrade or replace the wireless card.

In both cases, some devices will require an external network card or wireless card/dongle to be plugged into it to meet these requirements. Apart from ensuring that any plug in cards used are compatible with your device, there is no difference in how these external cards are configured or connect to the internet service.

Any device connecting to the internet service should be currently licensed and use a manufacturer supported version of its operating system. It is recommended that all security updates are applied and where it is considered 'good practice' for the type of device being used, that licensed, up-to-date antivirus software is installed.

Determining the suitability of a device for connection to the internet service is your responsibility, but almost all devices that are less than 5 years old and that meet the above requirements and that are correctly configured are likely to be able to connect to the internet service.

Where a room or accommodation unit has a wired connection, only one live connection is provided. If you have a requirement for connecting multiple devices you will need to obtain an active device to do this. There are 2 different options when using active equipment depending on the number of devices to be connected:

1. Where there is a requirement for connecting 4 or less devices to the internet service, an unmanaged switch is recommended as the simplest solution. These devices require no setup past connecting the switch to our network and connecting your devices to the switch.
2. Where there is a requirement for 5 or more devices to connect to the internet service, an Ethernet router or similar is recommended. The Ethernet router needs to be configured as the gateway to our network, with the devices to be connected to the internet service effectively hidden or masked behind the Ethernet router.

N.B. There is no limit on the number of devices that connect to the wireless service.

Unfortunately due to the vast number of these types of devices, we are unable to make specific recommendations for purchase, past using an Ethernet router, an ADSL router should not be used as

it is not compatible with the network. We are only able to provide very limited generic support for connection and configuration and this does not cover specific devices and their requirements.

In Halls of Residence where we have provided wireless in the rooms we ask that you do not install your own wireless routers and access points, as this interferes with our wireless equipment causing problems for users within the vicinity of your broadcasting wireless equipment.

Where a resident wireless router or access point is found to be causing interference with our wireless provision we may request that the device is turned off or preventing from broadcasting. If this request is ignored we may suspend the wired connection to which the wireless device is connected or formally request the removal of the interfering device.

So called 'passive' splitters should not be used. As although these devices will work, when 2 devices are connected the overall performance of your internet connection will be significantly degraded.

Conditions of Use

(a) General

Please be aware that by signing the Hall regulations form you are agreeing to abide by the following conditions of use and the JANET Acceptable Use Policy. JANET is the UK's research and education internet provider. A current copy of the JANET Acceptable Use Policy may be viewed or downloaded from: 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.

(b) Legal considerations

All users must comply with the terms of current relevant legislation, and in particular must not download, create, communicate to another person, or otherwise deal with any material which:

i) defames any person or any entity;
ii) is sexually explicit or obscene;
iii) is abusive, threatening, or racially offensive;
iv) infringes the copyright or violates the privacy of any other person;
v) infringes the rights of any person under the Data Protection Act; and/or
vi) is otherwise unlawful or objectionable.

Users should also note that 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.

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.

(c) 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.

(d) Complaints of Copyright Infringement

We routinely investigate all complaints of copyright infringement and they are handled in the following way:

1. 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.
2. 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.
3. 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.
4. 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.

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 1 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.

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.

(e) Potential for Harm
Users must not do anything that may cause or pose a risk of loss, damage, or significant expense to the University, or harm the reputation of the University. Care must be taken to ensure that any private statement made is not described as University policy, nor is in any way attributable to the University, and that all statements, especially those made in "public" messages, are not defamatory.

(f) 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.

(g) Privacy
The University routinely monitors all network traffic and stores all e-mail messages over its networks on the e-mail servers used. Thus, no e-mail should be considered to be completely private. The primary purpose of monitoring is for fault investigation. However, any anomalies may be investigated for possible breaches of terms and conditions of use, including illegal activity.

The University has the right to:

i) inspect network traffic between a user's machine and any other address(es);
ii) inspect e-mails, both incoming and outgoing, where the University has reasonable grounds to believe that a term of the University's IT policy has been breached; and
iii) take any action the University deems necessary, including limiting service or completely cutting off access, where it is considered advisable to prevent further misuse.

Except where monitoring provides evidence of a breach of these conditions or the JANET Acceptable Use Policy, or criminal activity, or significant cost to the University, information acquired will be kept strictly confidential to those involved in the investigation. In the case of criminal activity, the information will be made available to the police and the user's College.

(h) 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.

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.

(i) Support

The SWAN support team provide internet connectivity to the data point in your room and basic advice for connecting common devices to use the internet service. The SWAN support team do not provide general support for either hardware or software. The support team are also unable to provide support for devices that are using software that is not licensed/counterfeit.

All problems with the internet service should be reported to the SWAN helpdesk team who will open a helpdesk ticket for the problem and attempt to resolve the problem where possible over the telephone or by email. The helpdesk team can be contacted by telephone: 020 7862 8111 Monday to Friday
09:00 to 17:00.

Alternatively an email can be sent to swan.support@london.ac.uk any time. Please make sure that you note in your email some useful information to assist the support team, for example, your name, your hall, your room number, port number etc… A member of the SWAN helpdesk team will normally respond to any email sent the next working day, if sent outside of normal office hours. It is recommended that urgent or serious problems are reported by telephone where possible and non-urgent or minor problems are reported by email.

Where the helpdesk are unable to resolve a problem at the initial reporting stage, a member of the SWAN support team will contact you inside 5 working days to provide further support. The support team, where possible, will endeavour to better the 5 working day period. If deemed necessary, a member of the support team will come to your room and inspect your data point and/or your device where you have provided consent to do so.

At present, no support is provided outside of office hours, at weekends, during bank holidays or on University Closed Days.

If the internet service is used other than as authorised, the University reserves the right to terminate individual connections immediately and without notice. This is done to prevent further intentional or unintentional misuse particularly in cases where misuse is causing or is likely to cause loss of service to other users.