

Conditions of use of the Residences Network

As a member of the LSE using the network, you must still abide by the School's Policy Statement on the Use of Information Technology and the Conditions of Use of IT Facilities at the LSE when using the network in the halls of residence. In particular, you must not distribute offensive material, illegally copy software, breach copyright or send mass unsolicited email messages. In addition, the following conditions of use also apply.

Your attention is drawn to the fact that a failure to adhere to these conditions may result in the withdrawal of your access rights.

Connections

1. Residents may connect their network computing device to the network socket in their study bedroom. Network computing devices may only be connected to other network sockets where prior permission has been granted.
2. Wireless network access is provided by IT Services in the common areas of many Residences. Connection of any unauthorized wireless devices to the LSE network is forbidden.

Registration

3. Residents with a valid LSE username and password may register one network computing device for connection to the Internet and enhanced access to the LSE network from the Remote Support Activation page.
4. The connection to the registered devices is provided for the sole use of the registrant and must not be redistributed to others. The registrant is responsible for all network traffic to and from the registered network device.
5. Residents shall not alter any network configuration parameters assigned by or notified to LSE systems for their device unless specifically instructed to do so by a member of IT Services.

Availability

6. The default provision from wired network connections is web access to LSE email, the LSE and Library websites, the LSE Remote Desktop.
7. The network connection to study bedrooms is configured to give priority to the services most closely associated with academic study. This may adversely affect the performance of some social Internet applications.
8. IT Services will endeavour to provide a reliable and robust connection to the School network and the Internet, however, this cannot be guaranteed and acceptance of these terms and conditions in no way constitutes a guarantee of uninterrupted service.

Security and Monitoring

9. In order to detect and prevent potential or exploited network vulnerabilities, IT Services may perform regular monitoring, scanning, or probing of devices connected to the network. In using the network connection you are giving your consent to this activity and to the remedial actions described below.
10. Residents are responsible for the security of their own network devices. Security guidelines are available from LSE's Information Security pages. IT Services reserves the right to disconnect a network device if it is deemed to be a threat to security or in breach of policy.
11. A network installation of Sophos antivirus is available free of charge to current LSE staff and students. It is highly recommended, for the protection of all network users, that this software is installed. Residents who do not install Sophos may experience restricted internet access.
12. Residents may request that their own computer be scanned for vulnerabilities from <https://selfscanner.lse.ac.uk> and view their own results only. Installation or connection of any type of port scanner or packet sniffing technology to the LSE network for any reason is forbidden.

Remedial Action

The remedial action may be taken as a result of any of the following:

1. Regular monitoring of the volume of network traffic and other factors that may have an impact on network performance and reliability indicate that further investigation is necessary.
2. Receiving a complaint from an individual or organisation.
3. Scanning the LSE file servers for viruses indicates that further investigation is necessary.
4. Scanning the LSE file servers uncovers software that may pose a security risk to the network and/or other network users.
5. The use of "friendly probes" reveals security vulnerabilities.

Action(s) taken as a result of monitoring, scanning or probing could be any one or more of the following:

1. Notifying the user of a problem and requesting action to be taken within a stated period of time.
2. Further analysis of the source of network traffic to determine the nature of the suspected problem (e.g. high volume of network traffic being caused by file sharing programs and associated copyright infringement).
3. Deleting, removing, and cleaning of files on the LSE file server.
4. Disabling the network connection associated with the equipment.
5. Disabling the user's LSE account and making the user's H:Space accessible to IT Services only.