

Birkbeck, University of London

Malet Street, Bloomsbury

London WC1E 7HX

**Wireless Network Policy**

**Introduction**

A number of Wireless (Wifi) Access Points are available in Birkbeck for the connection of equipment being used by staff and students in the College. In addition, a guest wireless service is available for authorised visitors affiliated to Birkbeck. The objectives of this policy are to clarify responsibilities of users when using the service.

This policy applies to all wireless network devices utilizing Birkbeck IP address space and all users of such devices.

All users of the Birkbeck Wireless Network must accept the conditions of use contained within this policy, and other applicable policies including the Network Security Policy, Birkbeck Computer Regulations, Janet Acceptable Use Policy, eduroam guidelines, and any School policies which may be in force.  The following summary is from Birkbeck’s Computing Regulations:

* **Governance.** Don’t break the law, do abide by Birkbeck’s regulations and policies, and do observe the regulations of any third parties whose facilities you access.
* **Identity.** Don’t allow anyone else to use your IT credentials, don’t disguise your online identity and don’t attempt to obtain or use anyone else’s.
* **Infrastructure.** Don’t put Birkbeck’s IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.
* **Information.** Safeguard personal data, respect other people’s information and don’t abuse copyright material. Remember that mobile devices may not be a secure way to handle information.
* **Behaviour.** Don’t waste IT resources, interfere with others’ legitimate use or behave towards others in a way that would not be acceptable in the physical world.

**Using the Wireless Network at Birkbeck**

* eduroam is the supported wifi network for staff and students.
* Birkbeck will not accept responsibility or liability for any damage or loss of data to any machine while in transit or connected to the Birkbeck network.
* A valid ITS computer account (username and password) is required to use the wireless and fixed network.
* All IP addresses for the Birkbeck Wireless and Mobile network will be assigned by a DHCP service maintained by ITS for College wide services.
* Access to central, ITS-managed filestore or other restricted services, will be available via VPN only.
* Any breach of regulations may be reported to your Head of School or Department. In more serious or repeated minor cases, a breach of regulations may be dealt with under the Birkbeck’s disciplinary procedures.

**Responsibilities of users**

1. Users are responsible at all times for the security of their accounts, passwords, data and system.
2. A user will be held responsible for any breach of regulations carried out using a connection authenticated with their username. This includes action taken by others.
3. Users must not attempt to authenticate using another person’s or organisation’s credentials.
4. Users must not do anything that interferes with the operation of the wireless service. This includes using an unfair or excessive share of the available network bandwidth.
5. It is illegal and against Birkbeck regulations to copy or share movies, music, software and other copyrighted material without permission from the copyright holder. Users must not do this, whether intentionally or arising from a failure to correctly configure a file sharing program on your computer.
6. Users should use secure applications where possible, including but not restricted to https, ssh, sftp.
7. Users may not tamper with, install or operate Wireless Access Points.
8. Users must not allow equipment to act as a server of any kind.
9. Users must not invent network settings or host identities.
10. Users must not transfer network settings or host identities from one machine to another.
11. Users are responsible for any equipment connected to the system and for ensuring that it is in good working condition, and will therefore not present a health and safety risk to people or College property.
12. Users should ensure that operating systems are patched up to date.
13. Users should ensure that systems have up to date anti-virus software installed.
14. The use of the VPN service is recommended.
15. The use of a personal firewall product is recommended.
16. Users should report areas of poor wireless signal strength to allow us to extend coverage where needed.
17. Users must ensure that any equipment connected to the Service shall not be used for monitoring network traffic.
18. Users must not attempt to bypass network security or run any software designed to open unauthorised channels through the firewall. This includes but is not limited to software designed to tunnel traffic through HTTP proxies.
19. Users must accept and agree that a breach of the above terms may result in immediate withdrawal of the Service.

**Guest/Visitor Services**

1. Guest/Visitors from other organisations participating in eduroam are expected to use eduroam credentials provided by their home institution.
2. Other Guest/Visitor accounts are available to visitors to the College operating on Birkbeck business and sponsored by a Birkbeck member of staff.
3. Guest/Visitor accounts typically last between 1 and 5 days.
4. All user responsibilities stated above apply to Visitors/Guests.

**Authority and responsibility**

1. IT Services (ITS) has overall responsibility for Birkbeck's data communications and telephone infrastructure. ITS will therefore be responsible for the deployment, management and support of all wireless local area networks on Birkbeck premises.
2. No wireless LAN equipment (access points, bridges, etc) that is not under the direct supervision of ITS may be attached to Birkbeck's network. If Schools or research groups have teaching or research requirements involving wireless LANs that cannot be satisfied via central provision they may seek approval from the ITS Systems and Networking Team, or nominated individuals within Schools, to deploy wireless LANs in areas for which they have sole responsibility and a legitimate teaching or research requirement.
3. All Access Points and wireless client adapters on the Birkbeck Wireless LAN will use Service Set Identifiers (SSIDs) maintained by ITS.
4. IT Services reserves the right to firewall and restrict certain network traffic for the purpose of ensuring the security of Birkbeck networks.
5. ITS reserve the right to suspend access to the wireless network by any user in breach of this or other Birkbeck policy.

**Other information and applicable policies**

* [Details of the wireless and mobile service](http://www.bbk.ac.uk/its/services/wam)
* [Birkbeck Network Security Policy](http://www.bbk.ac.uk/hr/policies_services/policies_az/networksecurity)
* [Birkbeck Computer Regulations](http://www.bbk.ac.uk/hr/policies_services/policies_az/computing_regulationspdf)
* The [JANET Acceptable Use Policy](http://www.ja.net/services/publications/policy/aup.html)
* [eduroam (UK) Policy](https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-policy)
* Mobile Device Security Policy (for Staff)

If you have any questions, please contact the ITS Service Desk.