

METU Wireless Network - Rules and Regulations for Use

1. The use of wireless network resources (network connection, wireless network connection card, campus /off-campus access etc.), which are allocated for METU students and members, is subject to the rules and conditions set forth within "**METU Computing and Networking Ethics**" which is available at [this address](#).

2. The state allocates and grants to the University financial resources in order to accomplish essential computer networking technology investments that will primarily aid the instructional, academic, research and administrative objectives of the University. The personal use of the wireless network facilities by the users should in no way disrupt access priorities of those users that use the network for such **instructional, academic, research and administrative objectives**. In this respect, the users can find the **guidelines for the appropriate use of network resources, the rules and regulations** that the users must comply with and misconducts & prohibited behaviours as below:

- *KaZaA, iMesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, FastTrack, Audiogalaxy, MFTP, eMule, Overnet, NeoModus, Direct Connect, Acquisition, BearShare, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX, DC++, BitTorrent etc..*
- a. Peer-to-peer (P2P) file sharing programs, as well as violating copyright and licensing rules, use up an excessive amount of bandwidth that consequently hinders the use of network resources for purposes of priority. For this reason, it is strictly forbidden to use the "**peer-to-peer**" file sharing programs - even if they are used inside the campus network. Such usage includes, **but is not limited to**, the following programs:
- b. It is expressly forbidden to use wireless network resources for **commercial purposes or for activities of personal gain**.
- c. It is forbidden to use wireless network resources for **mass mailing, mail bombing, sending spam** and users are not allowed to provide the means to the third parties to perform similar acts.
- d. It is prohibited to keep possession of server computers that **provide internet service** (web hosting service, e-mail service etc.) via wireless network.
- e. Users must not intentionally **allow others to use University network resources from outside or, in other words, users must not pave the way for others to exploit privileges and act as if they are authorized to own the legitimate rights of the University users**. (proxy, relay, IP sharer, NAT etc.)
- f. It is forbidden to commit **activities that threaten the security of the network** (DoS attack, port-network scan etc.)
- g. Users are definitely not allowed to **change the hardware address** (MAC address) of wireless network interface. This address is only to be handled and verified to the authentication system of METU Computer Center (CC) by the CC Network Group. If changing the MAC address is inescapably required (as in the cases of breakdown or failure of wireless network access card etc.) users must certainly report it to Computer Center to carry out the proper procedure for that change. (The computer will not gain access to the wireless network, unless its new MAC address is authenticated by the authentication system).
- h. Wireless network facilities of the University (network connection, user codes, local/off-campus access etc.), which are granted as a privilege to the University members, will be used by every user in an appropriate, legal, ethical and considerate manner in accordance with the codes of behaviour and the regulations. It is the sole responsibility of all users that they are not endangering the safety of the resources by providing intentionally or unintentionally the means to **the third parties to access to network resources**. The user alone is answerable and accountable for every unlawful and unwanted consequences that may result from this act.

3. If the use of the computing and networking facilities is proven to be incompatible with the educational and scholarly missions of the University, and if the user has been proven to behave irresponsibly, inappropriately and illegally in a manner displaying disruptive and inappropriate conduct that endanger the efficiency, integrity, safety and continuity of networking services; and if the user breaches the rules and regulations set forth in this document, one or more of the following disciplinary actions may be taken as a reasonable response to eliminate threatening and abusive behaviour;

local and/or off-campus network access privileges may be restricted,

local and/or off-campus network access privileges may be suspended, modified or withheld,

the user codes and user accounts on the central server systems may be terminated,

University's disciplinary mechanisms such as investigation or prosecution may be initiated,

judicial proceedings may be started,

4. the student, who has been proven to have disregarded or violated the rules and regulations, will be forewarned the departmental secretary.

5. These rules and regulations become effective as soon as they are publicized. The University and Computer Center reserves **the right to amend these Rules and Regulations** at any time without prior notice. The **updated version of the rules and regulations** can be viewed at this web address.

NOTICE of DISCLAIMER:

METU CC does not accept any responsibility of the risks that arise from utilization of the wireless network. All responsibility belongs to the user