Internet Usage
Effective as of: 09.01.2021

American University of Armenia
Policy for Publication
Policy Number: ICTS20210007

---

1. Rules

Internet access provided by AUA including the use of the local area network and wireless network using college-owned equipment or a personal devices. The Internet is accessed through fast downlink channels providing fast Internet access. To access the Internet from the public library computers, the proxy server is used, requiring authorization whenever a user tries to access Internet from a web browser.

In case of having problems with Internet access an e-mail request must be sent the ICTS Department via the Intranet.

2. Available channels

The AUA has three downlink Internet channels. Whenever a channel is down a switching to alternative channel takes place. The switching between channels is done automatically.

During the switching, the Internet may be inaccessible for 4-5 minutes.

3. Academic freedom

The Internet is an important tool for members of the AUA community to use in exercising their academic freedom. Academic freedom is a core value for the AUA, and the use of or access to the Internet shall not be restricted for any community member who uses it in the pursuit of learning or free exchange of ideas, and who does not commit violations qualifying as Internet abuse.

4. Violations Qualifying as Internet Abuse

The Internet at the AUA must be used in a manner that is lawful, consistent with the mission of the AUA, consistent with AUA codes of conduct, and that does not compromise the security and effective operation of the network.

Prohibited uses of the Internet include, but are not limited to:

- Use of the Internet in a manner that violates copyright or intellectual property rights. If the AUA determines that such a violation has occurred it may take action under the Actions section below;
- Use of the Internet to disseminate unsolicited, mass distributed e- mail (spam) that is clearly unrelated to the mission of the AUA (e.g. pursuing of academic goals, carrying out of job responsibilities, or otherwise contributing to the healthy life of the AUA);
- Use of the Internet in a fraudulent manner. Such use may include, but is not limited to, the alteration or forging of e-mail headers or someone's digital signature, impersonation of another, or other actions designed to deceive;
- Use of the Internet for commercial purposes;
- Intentionally compromising network security or integrity. Such compromising of security or integrity may include, but is not limited to, attempts to circumvent user authentication; attempts to intercept or interfere with others' use of the network; intentional transmission of virus, worm, Trojan horse, or other code with malicious intent;
- Excessive use of the Internet for non-job related downloads.

5. Actions

- **Suspension or Termination of Internet and Network Access because of Internet Abuse**

The ICTS Department monitors Internet usage and subnets traffic. In case of the excessive use of bandwidth or any other misuse be detected, the Internet use may be suspended until the matter is resolved with the ICTS Director. The user is informed about that with an appropriate message.

- **Internet and Network Security Protection Emergency Measures**

The ICTS Department is allowed to take immediate action to preserve the security and integrity of the network should an acute threat arise. When such an emergency situation arises, The ICTS Department may suspend service, review log records, and take other actions as judged immediately necessary to protect the network. Great discretion must be observed in taking such measures, but the option is made available under this policy in order to allow the ICTS Department to preserve the network under exceptional circumstances.