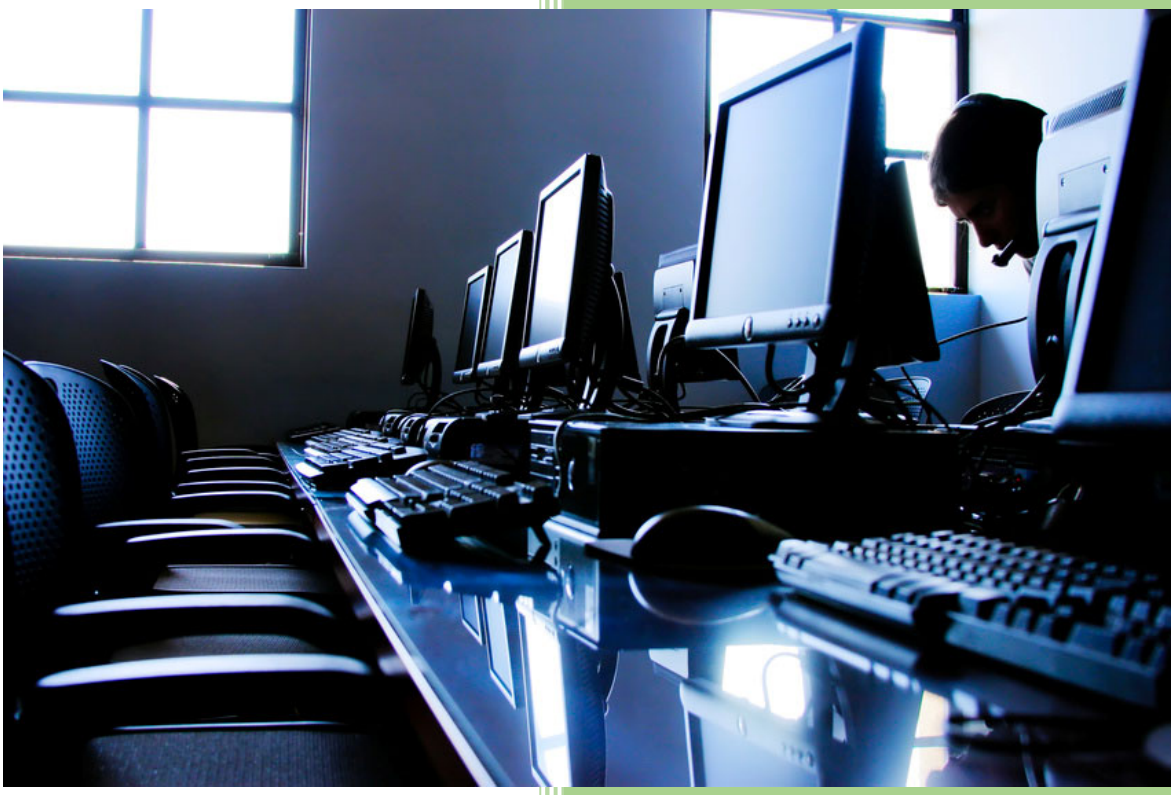
IADT Wireless Network Acceptable Usage Policy

Document Reference and Version No	Wireless AUP v4
Purpose	This policy relates to all users of IADT wireless networks
Commencement Date	April 2021
Date of Next Review	March 2024
Who needs to know about this document	All Staff, Students and external parties using the Institute's ICT Resources
Revision History	Minor revision on previous version
Policy Author	Head of Information Services
Policy Owner	Head of Information Services
Approval by Sec/Fin Controller	April 2021

Wireless Network Acceptable Usage Policy



Information Services Division

Dun Laoghaire Institute of Art Design and Technology

Contents

1.0 Overview

The ICT Acceptable/Appropriate Usage Policy (AAUP) specifies each IADT ICT Resource user is responsible for their use of technology be it on or off campus. The IADT Wireless Network Acceptable Usage Policy is an extension of this policy and gives more specifics around the use of this very valuable ICT resource.

2.0 Scope

These guidelines apply to all users of IADT wireless networks.

3.0 IADT Wireless Network Acceptable Usage Policy

3.1. Use of IADT's wireless network is subject to IADT General Regulations on the use of ICT, IADT's ICT A/AUP, HEAnet's AUP and any future AUP's produced by IADT or IADT's internet providers. The below policies and procedures are additional to those found in the policies referred to above.

3.2. This wireless network has been designed, built and maintained by the Information Services for the sole use of IADT staff and students along with EduRoam for staff and students from affiliated institutions. These in turn must have valid network account from either IADT or their home institution.

3.3. Performance and availability of the Wireless network will vary and cannot be guaranteed.

3.4. This wireless network is an unsupported service at a user level. It is not the responsibility of the Information Services to provide troubleshooting for users unable to connect or users having issues with computer hardware or software. The ICT Support Desk will not troubleshoot such issues other than to ensure the network is operational.

3.5. Security of devices connecting to this network is solely the responsibility of the user/owner. IADT's wireless networks, like WiFi networks in public places, are to be considered "un-secure network", this means that users of these networks must take their own precautions in protecting their device and data from any possible security risks. The three sub points below are guidelines for users to minimize security risks to themselves and other users of the wireless networks. It is not the responsibility of the Information Services to patch and update client devices, nor will it provide any software to provide security to a user of this network except Wi-Fi enabled devices owned by IADT.

3.6. All client devices operating systems (OS) should be properly patched with the latest security updates.

3.7. All client devices accessing the wireless networks should have the most up to-date anti-virus software. This will not be provided to any user by the Information Services; it is the responsibility of the user to acquire their own software licenses. Microsoft Defender is a free AV solution that is recommended by Information Services for Windows 10 based machines.

3.8. The Information Services recommends that user have a personal firewall installed on the client device, this will protect unwanted visitors browsing a user's data, pictures or worse.

3.9. The Information Services cannot be responsible for cleaning or removing infected client machines infected through the Wireless network. However if a user is comprising the

network or other networks then this user will be removed from the network immediately and without warning.

3.10. IADT's Wireless networks are not a wireless hotspot; all users have to be authenticated. Only IADT staff, students and EduRoam users with a valid logon account may access the wireless network resources. Logs may be used for assessing network problems or identifying unauthorized or unacceptable use of the wireless networks.

3.11. All data transmitted across the IADT's wireless network may not be encrypted and users should take their own precautions around this fact.

3.12. The wireless network's maximum data speed is less than 1/10th the speed of the campus wired network. Due to the lower speeds high bandwidth applications and websites, email websites (excluding IADT recognized email sites) and other websites maybe limited on this network. Access privileges will be subject to review.

3.13. All client wireless connections will go through a firewall for security, web monitoring and filtering software.

3.14. IADT under the obligations to HEAnet, and the wider web community is obligated to investigate any suspected illegal network traffic. Due to this commitment IADT retains the right to request access to a client machine if illegal activity is suspected to be emanating from this machine.

3.15. IADT retains the right to remove a user from the network without any prior warning and remove the whole network if necessary for any reason and without notice.

3.16. Broadcast frequencies used by the wireless network will be monitored on IADT property. Devices that interfere with the wireless network may be subject to restriction or removal.

3.17. IADT will provide access to HTTP and HTTPS.

3.18. There is no support for IPv6 on IADT wireless networks.

3.19. IADT will not be held responsible for any viruses, attacks, hacks malicious or otherwise or any loss of data that a user or their device connected to IADT provided wireless networks may experience or be subject to.

4.0 Further Information

If you have queries in relation to these guidelines, please contact:

Head of Information Services

Dun Laoghaire Institute of Art Design and Technology

Tel: 012394777

Email: ict_manager@iadt.ie