



Code: **QA439**
Title: **Wireless Access and Usage Policy**
Review Date: **September 2020**
Approval: **University Management Team (UMT)**

1. Purpose

The purpose of this policy is to establish a minimum set of criteria that governs access to the wireless network that includes permitted connections and the usage of such connections once established. The primary purpose of the policy is to ensure a more consistent measure of security, integrity and fair usage across the University's campuses.

2. Description

The policy applies to:

- All staff and students who wish to utilise the University wireless network
- All contractors, vendors or others (3rd parties), who wish to utilise the University wireless network.
- All visitors, guest or "in attendance" externals who wish to utilise the University wireless network.

3. Definitions

"**Must**", or the terms "**required**" or "**shall**", refer to an absolute requirement of the policy.

"**Must not**" or "**shall not**", refer to statements which are an absolute prohibition of the policy.

"**Should**" or "**recommended**" refer to a statement that should be applied. In certain circumstances, there may be a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.

"**Should not**" or "**not recommended**" mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.

SSID; Service Set Identifier, this is the name of the broadcasting WLAN (Wireless Local Area Network), i.e. the name of the wireless network which allows differentiation of wireless services. NUI Galway broadcast two services: eduroam and NUIGWifi.

4. Requirements

The following requirements apply:

1. All wireless access points on the NUI Galway network must be approved and centrally managed by ISS; non-sanctioned installation of wireless equipment is strictly forbidden.
2. All users must supply a valid set of credentials when attempting to connect to the wireless network.
3. Users must not attempt to circumvent or make changes to the security configuration of access points
4. All computer equipment and devices used to connect to NUI Galway's network must display reasonable physical security measures, i.e. devices must have a screen lock out setting and users must lock screens when stepping away from them.

5. NUI Galway reserves the right to analyse data gathered on the wireless network.
6. NUI Galway reserves the right to prioritise access to this critical service and reserves the right to implement bandwidth limitation to ensure a fair distribution of bandwidth across all users
7. NUI Galway, may, on formal request, assist law enforcement in relation to wireless use
8. NUI Galway reserves to the right to change internet filtering rules at any time.

5. Responsibilities

Name	Responsibility
ICT Security Committee Chair	Policy Owner
Director ISS	Revisions and updates to the policy
University Management Team	Approval of the Policy
All who use or have access to NUI Galway IT system	Responsible for implementation of the policy.
Internal and external audit	Monitoring and reporting compliance with the policy
ISS Service Desk	Tracking of calls related to Security Incidents

6. Related Documents /Attachments

Password Guidelines

QA406 Remote Access Policy

QA408 Logical Access Policy

QA411 End User Policy