Network Connection Guidelines – Last amended September 2016

The University operates networks within academic and support buildings, on campus student residences as well as certain private off campus accommodation. The University needs to manage and restrict certain devices from network connectivity where the device may downgrade the service available to the wider community, and thus apply to all of the aforementioned networks. The Director: I&TS or his/her nominee may permit individual exceptions to the following points on application.

Wired and Wi-Fi networks

1. Devices connected must:
   - use a consistent MAC address on each wired or Wi-Fi interface;
   - request IP address information dynamically:
     - IPv4 addresses must not be statically configured but be requested via DHCP
     - IPv6 addresses must not be statically configured but be requested via DHCPv6 or SLAAC, as indicated by Router Advertisement flags; and
   - run an operating system which is up-to-date and still maintained by its vendor.
2. Devices connected must not:
   - share or bridge the connection to the University network with another network interface.

Wired networks

3. The following types of devices may not be connected to wired network points:
   - network switches, routers or hubs;
   - wireless network access points or bridges; or
   - any device containing an embedded switch, router, hub or wireless access point, except where that function has been disabled.
4. Devices connected to wired network points must:
   - be connected using a patch lead no longer than 3m;
   - support 10 Mbps, 10/100 Mbps or 10/100/1000 Mbps Ethernet with autonegotiation enabled; and
   - be registered through an online registration process or, for devices which do not provide a web browser, manual registration on request.

Wi-Fi networks

5. The following types of devices may not be connected to University Wi-Fi networks (eduroam, Events@Rhodes):

    - network routers;
    - Wi-Fi network bridges, repeaters or signal boosters;
    - any device permanently fixed in place, including but not limited to data projectors, security cameras or access control devices (wired network connectivity should be used instead);
    - shared printers; or
    - desktop or laptop PCs which are used by multiple users, or imaged by I&TS.