IT Network Policy

1.0 Purpose

The College depends heavily upon its IT Network for research, teaching and administrative activities. It is essential that the stability, integrity and security of the IT network be safeguarded for use by all members of the College.

The IT Network is the infrastructure which connects devices allowing the exchange of data to support the College's business and operations.

The management and oversight of the IT Network is the remit of IT Services under the management of the Head of IT. The College reserves the right to refuse connection for any non-standard device.

2.0 Scope

The scope of the policy covers all users and all equipment irrespective of ownership that is attached to network data points on the College network or uses the College operated wireless network.

For the purposes of clarification, this includes, but is not limited to desktop computers, laptops, servers, printers, tablets, Chromebooks, smart phones, reprographic and audio-visual devices, irrespective of ownership.

3.0 Network and Device Compliance

To maintain the integrity and protection of the College's IT Network all equipment connected to the IT Network must comply with a set of minimum standards. Poorly configured, managed or operated equipment may lead to serious degradation of network operation or a breach in network and systems integrity resulting in:

- Disruption to business as usual processes
- Disclosure of college information
- System or network compromise

3.1. Permission must be obtained from IT Services before any non-standard device is connected to the network. This process is handled through the IT Service Desk.

3.2. The College may use an installed agent to control network access and ensure appropriate service packs and anti-virus programs are installed, up-to-date and running.

3.3. IT Services may employ measures to ensure compliance with this policy, the IT regulations and the associated policies e.g. remote audit and security penetration testing.

3.4. For security and network maintenance purposes, authorised individuals within IT Services may monitor equipment, systems and network traffic at any time.

3.5. All devices must use DHCP for IP configuration, with the exception of essential IT Infrastructure devices.

3.6. All users of the network must be aware of and abide by the College's Acceptable Usage Policy and the Jisc Acceptable Use Policy as operated by Jisc. The full text of their policy can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy.

3.7. New physical connections of equipment to a data port of the College's network may only be made by IT Services. Under no circumstance should a user attach any device to a data port. Any unauthorised device found attached to a data port will be removed and disposed of without warning.

3.8. Connected equipment must be maintained in accordance with manufacturers' recommendations. In particular, operating system and application software should be kept up-to-date to ensure that security vulnerabilities are not created. Systems must run up-to-date anti-malware software where available.

Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches, without the prior approval of the Head of IT Services.

3.9. Users must not attempt to circumvent any firewall or software designed to protect systems against harm.

3.10. Unauthorised use of IP addresses or changing of a System MAC address is prohibited.

4.0 Wireless Network

4.1. All wireless connections to the College network must be individually authenticated, logged, and be trackable back to the user.

4.2. All wireless access points which connect to the College network must be owned by the College and operated by IT Services. Users must not turn their device into an access point or an ad hoc network unless all devices on the ad-hoc network are isolated from the College's network.

4.3. Rogue wireless access points will be located, removed and disposed of by IT Services.

4.4. Personally owned Mobile Devices including any device not owned by the College is only authorised to connect to the WLC_OpenAccess wireless profile for Internet access only.

5.0 Firewall

5.1. All parts of the College network (i.e. all of the IP address space allocated) will be protected by a centrally managed College Firewall.

6.0 Disciplinary Process

The College reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the College's Disciplinary Policy. Disciplinary action may ultimately lead to dismissal.

7.0 Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Head of IT Services.