Connecting to the IT Network Policy

External version

This policy applies to any system/equipment that connects to the Cranfield University data network[1].

1. Scope

This policy covers, but is not limited to: desktop computers, laptop computers, departmental server systems, wireless devices and network layer equipment.

Network switches, routers, or other network equipment shall not be connected to the network or operated in a standalone mode, in the case of wireless network equipment, without prior consultation with the Information Services (IS) Professional Service Unit (PSU).

2. Requirements on Computing Equipment

Connected systems/equipment shall:

- Run anti-malware software that is regularly updated from a central or supplier-based system
- Run a supported operating system that is regularly updated and patched
- Run applications that are regularly updated and patched
- Have an Internet Protocol (IP) address that is supplied via a Dynamic Host Configuration Protocol (DHCP) reservation, unless otherwise agreed with the IT Service Desk
- Have valid licence agreement(s) for any installed software

Server operating systems and software should not be operated unless their use have been agreed with the IT Service Desk.

3. User requirements

Users of the equipment shall agree to:

- Abide by the University's rules and regulations:
  - University Laws - Charters and Statutes
  - IT Users Policy
- Allow authorised IS PSU staff[2] to inspect the equipment in the event of suspected misuse or network security related investigations

[1] The Cranfield University data network includes all school, PSU's, departmental, residential and sponsored networks that exist on any of the University campus sites.

[2] Authorised staff are defined to be: staff who belong to the IS PSU who have been authorised by the Director of Information Services or nominated Deputy(s).

4. User awareness

Users shall be aware that:

- Network traffic may be monitored to aid network trouble-shooting, problem resolution and in-line with legal and regulatory requirements
- Changes to computer configuration settings may be required if not consistent with University policy and standard operating procedures
- Equipment will be disconnected if it fails to meet the standards set in Section 2
- They take responsibility for incidents related to the use of their own personal computing equipment

5. Incident response

In the event of a system interfering with normal network operations, or where it is exhibiting unusual traffic flows or activities then:

- The specific system/equipment will be disconnected from the network, or
- The network segment or subnet, local to the offending system/equipment, will be disconnected from the network, and/or
- The registered owner of the system/equipment will be blocked from using University IT services

Restoration of services will only take place once resolution of the incident has occurred.

Document control

Document title	Connecting to the IT Network Policy
Document number	CU-IT-POL-2.01[E]
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Approval by and date	Information Assurance Committee; 21/09/2021
Date of last review and version number	September 2021; V1.7
Date of next review	August 2022
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.5	Wording amended to clearly state that equipment/users will be disconnected where inaction(s) would cause greater harm	Information Security	September 2019
1.6	Date and numbering amendments only	Information Security	September 2020
1.7	Date and numbering amendments only	Information Security	September 2021