# UCT network policy

## The UCT network as a core ICT service

### Document summary

| | | | |
|---|---|---|---|
| **Effective date** | 15 September 2009 | **Last updated** | 28 February 2011 |
| **Policy owner** | ICTS | | |
| **Approved by** | UICTC | | |
| **Enquiries** | ICTS | | |

### Table of Contents



### Background

At its meeting on 7 March 2005, the University Information and Communication Technology Committee (UICTC) approved the recommendation that the UCT network is a core ICT service. UICTC said that ICTS:

- will be responsible for ensuring compliance
- is to regulate the installation, management, and maintenance of all network devices
- has full power to ensure the security of the network and is to set standards of manageability
- will set standards for workgroups and end users to connect to the UCT network

UICTC further requested that ICTS set up a memorandum of understanding. This was adopted at the UICTC meeting on 8 June 2005.

### Purpose

This policy allows access to the above services, while restricting access to other services that are not widely required for academic purposes.

## Definitions

### 1. Types of devices

For the purposes of this document, three types of devices are defined as follows:

| Type of device | Definition | Example |
|---|---|---|
| End-user device | Any device intended for use by one individual at a time. | • Personal computers<br>• Laptops<br>• Workstations<br>• PDAs<br>• Mobile phones |
| Workgroup device | Any device configured to be used by more than one end-user for the purposes of sharing files, printers, scanners or other end-user devices. | • Servers<br>• HP JetDirect devices<br>• Network-aware scanners, copiers, printers, fax machines |
| Network infrastructure device | Any device intended to construct, extend, support, manage or secure a network. | • Routers<br>• Hubs<br>• Switches<br>• Bridges<br>• Wireless access points<br>• Firewalls<br>• Gateways<br>• Any workgroup or end-user device configured to perform the function of a network infrastructure device including proxy servers, network address translation devices, DHCP servers, remote access servers and DNS servers |

### 2. UCT network

For the purposes of this document, the UCT network is defined as:

- The data network that extends across UCT-owned or – leased premises excluding the Graduate School of Business.
- The network that connects various classes of devices to each other and to third-party networks such as the internet.
- Consisting of data cables and network infrastructure devices.
- From the average end-user's perspective, this includes the network up to the plug in the wall.

## Applicable to

All UCT staff, third parties and students that make use of UCT's network and its available services.

## Exclusions

All individuals that do not make use of UCT's network and its available services.

## Policy summary

This policy:

- describes the UCT network.
- defines the network as an enterprise-wide essential ICT service, that will, in the main, be owned and managed by ICTS.
- defines special purpose networks and top-up services.
- lists the next steps generated by the definition of the network as a core service.

## Policy details

All student residences will connect to the University network from behind routers that will also act as firewalls. These firewalls will be used to manage traffic to and from student residence networks. The following rule sets have been implemented on the firewalls between the UCT network and student residences:

### 1. The network is an enterprise-wide essential ICT service

1.1. UICTC has defined the network as an enterprise-wide essential ICT service. This means that UCT will hold ICTS accountable and responsible for the effective provision of this service. ICTS may impose limits on others only for the purpose of:

1.1.1. maintaining the integrity of the infrastructure.

1.1.2. making sure ICTS can meet its service level commitments.

1.1.3. implementing the key tenets of the ICT Strategy approved by Council (e.g. clustered redundant servers).

1.2. ICTS owns and manages the vast majority of the UCT network.

1.3. A key tenet of the ICT Strategy is that the network should be redesigned for high availability and monitored centrally. Maintaining the integrity of a campus network is particularly difficult since networks by their nature are subject to complex interactions. In principle, any device connected to the network may pose a threat to it*. Since most other ICT services rely on the network, the service level commitments on the network underpin all others.

*For example, devices incorrectly configured as DHCP servers have caused substantial downtime for large numbers of users.

1.4. It is vital that there is sufficient flexibility to meet the needs of teaching, learning, research, and administration. Specifically:

1.4.1. specialist research or teaching units may need their own separate, special purpose networks.

1.4.2. faculties or departments may have additional requirements that cannot be met within the central budget.

These cases are discussed below.

### 2. Special purpose networks

2.1. Some groupings may require separate networks due to the nature of their work. For example, a research group in Electrical Engineering may be researching network performance, and this might entail flooding the network with packets from time to time. In the case of special purpose networks:

2.2. In the case of special purpose networks:

2.2.1. The local network that serves the unit is defined as a third-party network, separated by a firewall from the UCT network. The firewall protects the integrity of the UCT network, while

allowing the unit access to specific services on the UCT network.

2.2.2. The firewall will be purchased by the unit, and installed, configured, managed, and monitored by ICTS.

2.2.3. The unit will be fully responsible and accountable for its special purpose network and for all associated costs.

2.2.4. ICTS service level commitments for network-reliant services will be ensured up until the firewall.

2.2.5. A formal agreement between ICTS and the unit must lay out the exact terms, conditions, and constraints.

2.2.6. All requests for special purpose networks are to be brought to the University Information and Communication Technology Committee (UICTC) for ratification. The exception is Computer Science, which UICTC has already agreed meets this definition.

## 3. Top-up services

3.1. Top-up services are additional network services or additional technical requirements that either cannot be met within the central ICTS budget or that are not appropriate to fund centrally.

3.2. The goal is to allow departments and faculties the flexibility that they need, while maintaining the integrity of the infrastructure.

3.3. In the case of top-up services:

3.3.1. ICTS is responsible for acquisition and approval of equipment that must conform to UCT network standards, including vendor choice.

3.3.2. The department or faculty is responsible for the costs of purchase, installation and maintenance but ICTS holds management responsibility for installation, configuration and maintenance. All costs must be made visible to the Planning and Budgeting cycle.

3.3.3. ICTS is accountable and responsible for the provision of the top-up service, including the management and maintenance of all devices and cabling.

**EXAMPLE**: A department may wish to ensure complete wireless coverage of all its spaces. While ICTS agrees that this is desirable in the long term, the central budget is not sufficient to meet this requirement. Should the department purchase devices without consulting ICTS, the department could inadvertently choose equipment that cannot be integrated with the rest of the infrastructure, cannot be managed effectively in order to maintain service levels, or that poses a security risk to the network.