Network Connection Policy

This policy applies to staff, students and all other users of the University of Dundee network.

Approved by: Network Improvement Programme Board, 19 May 2006

1.0 OBJECTIVE

These policies are required to enable the University's network to operate securely and reliably to offer a dependable environment for the University's communication processes and data storage. The University's Information & Communication Services (ICS) has been given end-to-end responsibility for, and control of, the network. This means that the wall socket and everything behind it belongs to ICS and is not to be accessed by non-ICS staff unless specifically authorised by ICS. Equipment belonging to Schools or Units may be plugged into the wall socket subject to policies and restrictions (e.g. 'Permission to Connect') as described below. This document defines the policies for management and use of the network infrastructure implemented through the Netcomms project, which apply until further notice.

2.0 SCOPE

This document applies to all use of the University network from end-to-end across all campuses and University residences, and includes all systems and devices connected to the network. Specific exceptions to these policies may be considered where appropriate. These will be covered by a signed agreement and documented on the ICS web site.

3.0 AUTHORISED USERS

Only authorised users are permitted to connect to and make use of the University's data network. These are the current categories of authorised user:

- Someone who is properly registered in the University eDirectory and who is
  - a valid member of staff, honorary member of staff or associate member of staff or
  - a matriculated student or an associate student or
  - a properly authorised and registered Associate User or
  - a registered visitor who has agreed to accept the relevant University rules and regulations
- Someone making legitimate use of the JANET Roaming Service (part of the eduroam federation).

Only a specific person is authorised; access must not be made available to friends, family members or anyone else. It is unacceptable for users to divulge their password or to allow unauthorised individuals to use it or any facilities to which it gives access. University regulations and acceptable use policies must be observed. [These are available from www.dundee.ac.uk/ics/pubs]
4.0 PERMISSION TO CONNECT

Only devices which have been given "Permission to Connect" may be attached to any part of the University's network. The following categories are currently defined with further details below:

1. **Standard devices**: Automatic permission to connect for PCs Apple Macs and laptops which fulfil the specified criteria
2. **IPT handsets**: Have automatic permission to connect as long as they are supplied by the University for use with its IPT system
3. **Data Network equipment**: Prohibited
4. **Wireless access points**: Prohibited
5. **Servers**: Require individual approval with agreed configuration and management
6. **All other devices**: Considered on a case by case basis

4.1 Standard devices
- **Connection**: Automatically given Permission to Connect
- **Scope**: Standard PC, Apple Macintosh, laptop, PDA
- **Obligations**: Must have all relevant security patches installed reasonably soon after release Must be running anti-virus software with up-to-date signature files Anti-spyware software recommended Automatic update of all these items is strongly recommended. Full details will be published on ICS website
- **Security**: Restricted to the use of a small set of essential services No incoming connections allowed from the Internet (but if your PC is running a softphone it can accept incoming phone calls)

4.2 IPT Handsets
- **Connection**: Automatically given Permission to Connect
- **Scope**: All IPT handsets provided by ICS. (For softphones see 1. Standard devices)
- **Obligations**: The handset must be managed by ICS
- **Security**: A tailored security design is applied to all IPT handset connections by ICS

4.3 Data Network Equipment
- **Connection**: Prohibited - no such devices may be connected [except by specific agreement]
- **Scope**: All network equipment such as switches, hubs, routers or any device which acts in such a capacity (e.g. a PC configured as a router). Network Address Translation (NAT) boxes are specifically prohibited.

4.4 Wireless Access Points
- **Connection**: Prohibited - no such devices may be connected [except by specific agreement]
- **Scope**: Any device which has a connection to the University network and which allows other equipment to make a wireless connection to it

Wireless Access Points offer a significant security threat because they can allow unauthorised access which is almost impossible to detect. They risk interfering with University wireless coverage because the number of channels is limited and has to be carefully controlled to reduce interference effects. ICS may be able to install additional wireless network access points at cost. Requests for advice can be made through the ICS Helpdesk.
4.5 Servers
Connection: Require explicit Permission to Connect
Scope: Any system which provides services and requires special security measures
Email gateways (SMTP servers) are included
Obligations: Must meet agreed security standards and be managed by an identified person
who will take appropriate responsibility
Must have all relevant security patches installed reasonably soon after release
Must be running anti-virus software with up-to-date signature files
Automatic updates are strongly recommended.
Security: Firewall and other security measures will be tailored to requirements as agreed
Incoming connections from the Internet can be tailored to requirements as agreed

4.6 Connection of all other devices
Special consideration will be given to lab equipment etc.
Devices will be required to meet security standards for operating system security patch levels
and for industry standard Anti-virus software with up to date signature files. Network
equipment (e.g. switches, hubs) may not be connected to the network, other than by ICS.

5.0 UNAUTHORISED MODIFICATIONS
Network equipment is stored in network cabinets in equipment rooms. Only those who are
specifically authorised by ICS may have access to the network cabinets and make any
changes. Only network equipment supplied and installed by ICS may be connected to the University network. This covers all repeaters, switches, routers, wireless access points and
any device similar to these. There must be no modifications to any such equipment without
prior approval of ICS. Requests for change such as the connection of additional switch ports
can be made through the ICS Helpdesk.

6.0 USING DHCP
All connected devices must follow best practice guidelines by using DHCP appropriately:
1. Every device is allocated an IP address
2. Every system should pick up their IP address via DHCP
3. The only exceptions should be systems unable to use DHCP
4. Every IP address is recorded in the DHCP tables whether statically or dynamically assigned
DHCP systems are centrally provided but an agreement may be reached to allow local IT support staff to update the tables.

6.0 NEW BUILDINGS & REFURBISHMENTS
- All installations for network cabling, equipment (and telephones) must conform to University standards.
- ICS must be consulted at the planning stage so that design and provision can be considered for approval well before building plans are completed.
- New Builds and Refurbishment projects will continue to budget for all network cabling, connections and network equipment required to establish the required services.
8.0 NETWORK UPGRADES & REPLACEMENTS

- All changes and upgrades, additions or replacements to University networks can only be undertaken by ICS.
- There should be early consultation so that design and standards can be considered well before work commences.
- Some elements incur a charge to cover costs incurred.

9.0 SECURITY

Security of the network is a high priority for the University. Management of security requires compliance as follows:

- Firewalls and access control lists are used to control network traffic
- A "Default Deny" policy is used so that only known acceptable traffic is permitted
- Only devices given "Permission to Connect" are authorised to connect to the network
- Servers and other devices requiring more than the standard access must be registered with ICS
- All traffic and systems may be monitored for a variety of reasons subject to University policies
- All systems on University network may be subject to vulnerability assessments with appropriate follow-up action taken to block access to compromised systems.

10.0 NETWORK CABLING INFRASTRUCTURE

- All cabling work must be authorised and approved by ICS in advance.
- In most cases, either Estates & Buildings or ICS will commission and manage any additional cabling installations. Work is undertaken to agreed University standards with 25 year guarantees.
- Requests for cabling work can be made through the ICS Helpdesk.

11.0 ADVICE & ASSISTANCE

Requests for advice and assistance about any matters covered in this document can be made through the ICS Helpdesk.