

Network Connection Policy

Paper D

This policy applies to all users of the University of St Andrews network.
Version 1.5, July 2008.

1.0 OBJECTIVE

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

2.0 SCOPE

This document applies to all use of the University network from end-to-end, 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 between IT Services and the party/ies involved. The Residence network (ResNet) is covered by separate policy.

3.0 AUTHORISED USERS

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

- Users who are listed in the University's LDAP directory and who have agreed to the University's terms and conditions and been issued with a personal username and password, provided that they are in one of the following groups:
 - members of staff, including honorary and retired staff and visiting scholars, who have a current contract with the University and who have been issued with a staff number by HR
 - students who are registered on a current course in the University
 - external users who have been sponsored by a current member of the University staff confirming that they are currently engaged in collaborative work with members of the University
- Temporary visitors to the University who have agreed to accept the University's terms and conditions, have provided proof of identity and been issued with a temporary username and password (valid for a

period not exceeding nine hours)

- Users 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.

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 Director of IT Services' decision to provide "Permission to Connect" or otherwise is final. The following categories are currently defined with further details below:

1. **Standard devices:** Automatic permission to connect for PC, Apple Mac, Linux devices which fulfil the specified criteria.
2. **Data Network equipment:** Prohibited
3. **Wireless access points:** Prohibited
4. **Servers:** Require individual approval with agreed configuration and management
5. **Printers:** Require type 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, Linux machine, laptop.

Obligations: Must be running a version of the operating system currently supported by its manufacturer, or supplier. Must have all relevant security patches installed reasonably soon after release. Must be running anti-virus software with up-to-date signature files if appropriate. Automatic update of all these items is strongly recommended. Must have strong passwords. Must not be in shared areas such as Common Rooms, Libraries, etc.

Security: No incoming connections allowed from the Internet, and no services may be provided by any device connected under this heading. (See Appendix)

4.2 Data Network Equipment

Connection: Prohibited - no such devices may be connected [except by specific written 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.

4.3 Wireless Access Points

Connection: Prohibited - no such devices may be connected to the network, or otherwise used within any University building. [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, or uses the frequencies allocated to 802.11 wireless networking.

4.4 Servers

Connection: Require explicit written Permission to Connect.

Scope: Any system which provides services. (file, print sharing, web pages, etc)

Obligations: Must meet agreed security standards and be managed by an identified person who will take appropriate responsibility, in conjunction with IT Services. IT Services must be confident of the security of the system as a whole. Must have all relevant security patches installed reasonably soon after release Must be running anti-virus software with up-to-date signature files if appropriate Automatic updates are strongly recommended.

Security: Firewall and other security measures may be tailored to requirements as agreed. Incoming connections from the Internet may be tailored to requirements by agreement with IT Services.

4.5 Printers

Connection: Require type approval for Permission to Connect.

Scope: Any device providing print output, and connected to the network, or any device connecting a non-networkable printer to the network, eg USB-to-Ethernet print server.

Obligations: Must meet security standards, and provide only print services, on standard ports. To be configured only as approved by IT Services, and configuration approval is material condition of Permission to connect. Must have recent version of firmware, and strong administrator password, copy of which held by IT Services. (See Appendix)

4.6 Connection of all other devices (e.g. Experimental Systems, BMS systems, IP CCTV cameras, Access Control, Machines in Public Areas) Special consideration will be given to lab equipment etc, for which no upgrade path is available. Devices will be individually assessed, and approval will be given in writing where appropriate. Devices will be required to meet security standards for operating system security patch levels, authentication, and for industry standard Anti-virus software with up to date signature files where appropriate.

5.0 IP ADDRESSING and REGISTRATION

All IP addresses must be assigned by IT Services, or a delegated third party. All devices on the network must be registered with IT Services, either by contacting the helpdesk to request a change to our records, or by

a delegated third party. Any device must use only the IP address assigned to it by IT Services, in the manner in which it is assigned by IT Services (Static Assignment, or DHCP).

6.0 UNAUTHORISED MODIFICATIONS

Network equipment is stored in network cabinets in equipment rooms. Only those who are specifically authorised by ITS may have access to the network cabinets and make any changes. There must be no modifications to, or any tampering with any network equipment without prior approval of ITS. Requests for change such as the connection of additional switch ports can be made through the ITS Helpdesk.

7.0 NEW BUILDINGS & REFURBISHMENTS

- All installations for network cabling, equipment (and telephones) must conform to University standards, (University of St Andrews Data and Telephone cabling specification, available from ITS or Estates.)
- ITS Infrastructure and Technical Services must be consulted at the planning stage so that design and provision can be considered for approval well before building plans are completed.
- The cost of all network cabling, connection and network equipment installed to provide network services in new or refurbished buildings will be charged against the budget of the relevant new build or refurbishment project.

8.0 NETWORK UPGRADES & REPLACEMENTS

- All changes and upgrades, additions or replacements to University networks can only be undertaken by ITS.
- 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, and are managed by IT Services
- 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 IT Services, and have written "Permission to Connect" from ITS.
- All traffic and systems may be monitored for a variety of reasons subject to University policies.
- All systems on the University network may be subject to vulnerability assessments with appropriate follow-up action taken to block access to

- compromised systems.
- Any machine found providing unauthorised services may be disconnected from the network, and disciplinary action taken against the registered owner of the machine.
- IT Services reserves the right to take any action that it deems appropriate to ensure the security and integrity of the University Network.
- The University reserves the right to take appropriate action against anyone found in breach of the stated policies.

10.0 NETWORK CABLING INFRASTRUCTURE

- All cabling work must be authorised and approved by ITS in advance.
- In most cases, either Estates or ITS will commission and manage any additional cabling installations. Work will be undertaken to agreed University standards, by IT Services approved contractors.
- IT Services must inspect and approve data installation work before the University accepts it
- Requests for cabling work can be made through the Telephone Office.

11.0 ADVICE & ASSISTANCE

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

APPENDIX

This policy has been formulated to allow IT Services to provide a safe, secure environment for networked computing in the University.

There are a number of other documents that should be read in conjunction with this policy, which provide clarification of policy that is referred to in this document.

Relevant material includes:

- Conditions of use of Computers in the University
- Procedures for setting up of computers
- Policies on email, web and computer accounts
- Email policy
- The Regulation of Investigatory Powers Act
- The Data Protection Act
- The IT Services Core Services Document

Some of the reasons for prohibiting connection of certain types of devices follow:

Users attaching unauthorised devices to our network cause a number of serious security threats.

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.

Network printers are rapidly becoming powerful computing devices in their own right. However, not all manufacturers are keeping pace with security developments, and we find that it is common that the firmware of these devices is not kept up to date, nor are they correctly configured. By type-approving devices, formulating correct, secure configurations, and managing firmware updates, we can significantly reduce the risks associated with such devices.

As for unauthorised devices, unauthorised services cause major issues, which could include unauthorised access to devices, or data held by the University.

Under item 4.1, to gain automatic "Permission to Connect", it states "No incoming connections allowed from the Internet, and no services may be provided by any device connected under this heading."

This means that these devices will not be allowed to provide any networked service.

A service is any process running on the machine that causes any user to be able to connect to it from any other machine, for any purpose. Simple examples of network services are: file sharing (shared drives), remote desktop, printer sharing, web servers, secure shell servers.

As none of these devices are permitted to run any such services, no incoming traffic whose connection originated outside the University will be permitted past the external Firewall. This will not affect access to the internet, rather access from the internet. IT Services may also apply appropriate restrictions on traffic originating within the University. This is explained in Section 9 of this policy.