NETWORK CONNECTION POLICY VERSION 1.1

Table of Contents

1. Statement of Policy 4
2. Background 4
3. Appropriate Devices 4
4. Making an Approved Connection 5
5. Connection to a Wired Network Managed by Information Services 5
6. Connection to the Wireless Network Managed by Information Services 6
7. Networks within the University not managed by Information Services 6
8. Designated Departmental Networks 7
9. Approved Private Networks 7
10. IP Address Management 8
11. Connecting Critical Systems to the Network 8
12. Disconnection from the Network 9
13. Other Relevant Regulations 9
14. Liabilities 10
15. Future Review 10

1. Statement of Policy

"No device may be connected to any of the University's wired networks without the approval of the Information Services Network Manager."

This document describes how appropriate devices may be routinely connected to the network in approved ways. Connection of other devices is either forbidden, or must first be authorised.

2. Background

The University of Strathclyde provides a pervasive modern data network infrastructure, designed to deliver a robust and reliable network service to all users

The network infrastructure is fundamental to all aspects of the business of the University and the foundation of all IT facilities across the University. In order to be able to deliver a reliable service, it is essential to ensure that:

Only appropriate devices are connected to the network;

Connection of any such device is made in an approved way.

Such connections are considered to be "routine". Connection of other devices, or connection in non-approved ways, is considered to be "non-routine" and hence unauthorised, and must be discussed with the Network Manager.

Unauthorised additions and modifications to the network infrastructure can cause service disruption to network users, particularly if incorrectly specified, ill-configured, or sub-standard equipment is used. Such service disruption may occur elsewhere on the network, not necessarily in the vicinity of the inappropriate device, and tracing the source of such disruption can be time-consuming in both effort required and consequential lost working hours.

3. Appropriate Devices

Only devices designed to operate as Ethernet "end nodes" may be routinely connected to the network. This includes, but is not limited to, personal computers, printers, etc.

There may be additional considerations for the connection of certain classes or types of device: for example, building management systems, security systems, till systems, etc. The connection of such devices should first be discussed with the Network Manager.

Under no circumstances should any non-"end node" device be connected to the network infrastructure, without the prior and explicit written permission of the Network Manager. This includes, but is not limited to, repeaters, bridges, hubs, routers, or any system with multiple network interfaces which may be configured to bridge, forward, route or relay traffic between those interfaces.

It should be particularly noted that no wireless access point (base station) may be connected to any network within the University, including non-Information Services networks and private networks (as defined below), without the authorisation of the Network Manager. This restriction is essential for security purposes, and to maintain manageability of radio frequency allocations – radio waves do not respect departmental political boundaries.

4. Making an Approved Connection

The connection of appropriate devices to the University network infrastructure may be made in the following ways:

To a wired network managed by Information Services Directorate

To a wireless network managed by Information Services Directorate

To a “designated departmental network”

To an “approved private network”

By connecting any device to any of the above networks, the user is accepting that, if considered necessary by the Director of Information Services, that staff working under his authority may examine and audit that device. It should be pointed out that the University Policy on Use of Computing Equipment and Facilities, states that the above condition applies not only to University-owned computers and devices, but also to privately-owned equipment, and equipment owned by a third party.

A network address (“IP address”) will ordinarily be required to be obtained and configured on each device. The means of doing so will vary depending on the network to which the connection is being made. IP address management issues are discussed in section 5.

IP address assignments have two types: “fixed” (or “static”), where a particular device is permitted to use the same address indefinitely, and “dynamic”, where a particular device will receive a lease to use an address for a fixed period of time, and must periodically request a new lease (this process is handled automatically).

5. Connection to a Wired Network Managed by Information Services

Information Services install and maintain the vast majority of network connections across the whole University. Most connections to a wired network will fall into this broad category. Connections must be made with a cable of the appropriate type; Information Services can provide guidance.

There are several classes of wired network, each with slightly differing requirements;

Primary Service Wired Network in Academic and Administrative Buildings

This is the most common class, generally intended for the connection of devices to be operated by University workers.

A fixed IP address must be assigned to each device by the IT Helpdesk or local IT support function. It is recommended that the device configures its IP address using the DHCP service, however if this is not possible it may be configured manually.

Wired Network in Halls of Residence

Ordinary residents of the Halls of Residence may connect an appropriate device to the wired network.

A device must be configured to receive a dynamic IP address via the DHCP service; it must not be configured manually.

Plug-in Wired Areas

Some areas have been designated as “plug-in” areas, for the short-term connection of wired devices. These are principally in areas where students may congregate, and largely pre-date the provision of wireless infrastructure. Some areas may be available for general “public” access while some may be restricted to users from particular departments.

A device must be configured to receive an IP address via the DHCP service; it must not be configured manually.

6. Connection to the Wireless Network Managed by Information Services

A wireless network extends to many parts of the University estate, and is available for use by any authorised user. Authentication is required to gain access; various methods of authentication may be available in order to obtain different levels of service.

A device must be configured to receive an IP address via the DHCP service; it must not be configured manually.

7. Networks within the University not managed by Information Services

There are a small number of networks within the University which are managed by other organisational units, not by Information Services. Information Services provides and manages a point of connection for these networks to the campus backbone. These private networks can be classified into two groups:

8. Designated Departmental Networks

A *designated departmental network* is a network autonomously managed by a recognised organisational unit within the University, and which has been approved by Information Services as suitable for connection to the University networking infrastructure.

The organisational unit must appoint an individual to be responsible for the day-to-day operation of the network, and to be the point of contact for Information Services.

Information Services will maintain the connection to the department and in some cases may be responsible for the physical cabling within the department, but will not be responsible for support of individual users or maintenance of active networking equipment within the department.

9. Approved Private Networks

An *approved private network* is a network owned and operated by a legal entity separate from the University (even where that entity is wholly owned by the University), and which has been approved by Information Services as suitable for connection to the University network infrastructure. A formal contract with the University will ordinarily be required to be established, and fees may be payable.

The entity involved must appoint an individual to be responsible for the day-to-day operation of the network, and to be the point of contact for Information Services.

The connection to the University network will be made according to these conditions, unless separately negotiated:

The physical interconnection between the networks will occur at a single Ethernet port on University network equipment - this is the “point of connection”; Information Services will have the sole management rights to this port;

- A layer 3 (routing) device will be connected directly to the point of connection – this is the “interconnecting device”;
- The network owner is responsible for any capital and recurrent costs associated with the interconnecting device;
- The network infrastructure does not share any Information Services equipment or wiring areas;

The users of the network abide by the relevant rules and regulations pertaining to the use of the University's network infrastructure, and those of JANET. In particular:

JANET Acceptable Use Policy

JANET Security Policy

JANET Terms for the Provision of the JANET Service

Information Services only provides service guarantees to the point of connection.

10. IP Address Management

A network address ("IP address") will ordinarily be required to be obtained and configured on each device.

In most cases, IP addresses are assigned (or "leased") to devices by Information Services or the organisational unit operating the particular network in use. They remain the property of the leasing organisational unit, and may be withdrawn or re-assigned at any time, although this will ordinarily be done in a manner which is not disruptive to service, except in extremis.

For example, it may be necessary to re-assign addresses to accommodate topology changes, or to withdraw addresses from devices believed no longer to be in use.

Under no circumstances should any IP address other than that assigned to the device by the appropriate mechanism be used; nor should IP addresses be "guessed". Devices discovered using IP addresses not allocated for their use by the appropriate mechanism are liable to be disconnected.

Where a fixed IP address assignment is no longer required (perhaps because the device has been permanently removed from the network), the IT Helpdesk or local IT support function should be notified, so that the address can be re-assigned to another device.

IP address assignments which appear no longer to be in use over an extended period of time may be withdrawn and made available for re-assignment to other devices. In that event, the registered keeper of the device or another recognised contact will ordinarily be informed.

11. Connecting Critical Systems to the Network

The rules described in Section 3 apply to the connection of all types of appropriate devices of a generic commodity nature to the network. Usually there will be no need to notify Information Services of the connection, other than by applying for an IP address where required. However, connection of some devices may have additional considerations; whether because they require a higher bandwidth connection, or the device is performing some important function (for example a departmental server or building management system).

In this event, the relevant parties are strongly advised to discuss the connection with Information Services, who will be able to discuss more appropriate connection strategies. For example, it may be beneficial to connect devices such as web servers or file servers closer to the core of the network, which may offer higher bandwidth, lower latency, or a greater deal of resilience and robustness. It may also be possible to provide such systems with a higher level of routine monitoring.

12. Disconnection from the Network

Information Services' first priority is to protect the business functions of the University and, in this context, this means to protect the network infrastructure from disruption.   If it is suspected that a device is causing disruption, Information Services would normally work in cooperation with recognised computing staff and/or the registered keeper of the machine to identify and resolve the problem.

There are occasions where the above approach is impractical – for example:

- The keeper of the device may be unavailable;
- The keeper of the device may be unable or unwilling to provide assistance;
- The device may be being used maliciously by a third party;
- The device may be causing problems elsewhere on the network as a result of mis-configuration or malfunction.

Under these or similar circumstances, Information Services may isolate the system from the campus backbone network, either by physically disconnecting it, or disabling the network port, or applying traffic filters in the network infrastructure. Users must not make any attempt to re-connect such a system unless they have received explicit instructions to do so from Information Services.

13. Other Relevant Regulations

This policy relates only to the connection of devices to the network. Once any devices have been connected in an approved way, the "University Policy on the Use of Computing Facilities and Resources" governs use of these devices.

University Policy - Use of Computing Facilities and Resources

14. Liabilities

As earlier stated, Information Services' first priority is to protect the business function of the University. In order to commit to the service availability required by the University, Information Services must ensure that not only is the network infrastructure free from disruption, but that it is free from potential disruption. It cannot do so if unauthorised devices are connected to the University's network infrastructure. Thus, any unauthorised equipment, wiring or network may be disconnected immediately, whether it is causing an immediate problem or not. Information Services will not reverse any such disconnection until proper procedures are followed and the risk negated.

Any department or unit connecting or authorising a connection, which has not been approved by Information Services, to the University's network infrastructure may be liable for the cost of bringing the connection up to an approved standard before reconnection can take place. This may include hardware costs, Information Services staff-time, and possibly sub-contractor costs. (End systems that have conformed with the Information Services recommended procedures and specifications, which have connected in good faith to existing infrastructure will not incur financial penalties if found to be faulty.)

15. Future Review

This policy should be reviewed every two years.