University of Aberdeen Network Connection Policy

1. Overview

The University's data network forms a critical part of the business infrastructure used to access business systems and data stores as well as carrying email and telephony. As such it is essential that this resource is carefully managed to ensure its capacity, availability and integrity. The demands placed upon the University's data networks are such that a single network is not able to meet all these needs, therefore there are several networks designed of provide the required service in each area.

Nothing in this document should be taken to override the University of Aberdeen *Information Security Policy* or the JANET Acceptable Use Policy. Where there is any conflict the above documents take precedence.

2. Purpose

The purpose of this policy is to define what can be connected to the University's networks and the standards that must be adhered to by devices so connected.

It covers:

- Who can connect devices to a network
- What devices can be connected to a network
- Ensuring appropriate management of network resources and network address space
- Auditing of this policy
- Enforcement action

Details of permitted activities by network connected devices are covered in the University of Aberdeen *Conditions for using IT Facilities* and the associated *Notes for Guidance*.

3. Scope

This policy applies to any device directly connected to any of the University's networks by any means (e.g. network cable or wireless). It does not cover remote access from out with the University. It also applies to anyone connecting or using a device connected to the University's networks including Staff, Students, Contractors and members of the General Public for whatever purpose that device is to be connected to the network.

The process of connecting a device to the network includes:

- Configuring the network to allow the device to communicate
- Physically connecting the device to the network
- Configuring the device to communicate on the network

4. Policy

Common policy applying to ALL University of Aberdeen Networks

Who

- In general only staff authorised by the Director of IT Services are permitted to configure or extend any University of Aberdeen network.
- Each network has a separate policy on who can physically connect devices to it. Details are given in the sections below.
- Each network has a separate policy on who can configure devices to communicate on it. Details are given in the sections below.

What

- Each network is provided for a specific purpose and only devices consistent with that purpose may be connected.
- Devices may be categorised as:
    - **Network equipment –** Such as routers, network switches, Wireless Access Points etc.
    - **Client Devices**
        - University owned: User Workstations, PCs, laptops, Mobile phones etc.
        - Non University owned: User Workstations, PCs, laptops, Mobile phones etc.
    - **Servers** – Devices whose primary purpose is to provide services to other network connected devices
    - **Network Printers and MFDs**
    - **Embedded devices** – Such as CCTV cameras, building monitoring systems etc.
    - **Other equipment** – Such as scanners, scientific instruments and Videoconferencing equipment.
- The connection or configuration of network equipment is considered 'configuring the network' and is only permitted by explicitly authorised staff. Authorised staff may delegate specific tasks in specific circumstances, e.g. consultants working on behalf of the University, however they remain responsible for such work.
- Any device connected to the network must meet the following minimum criteria:
    - Has a Network Interface Card capable of connecting to Ethernet Networks or 802.11 wireless networks.
    - Is capable of communicating using TCP/IP v4 network protocols.
    - Complies with current Health and Safety requirements, including Electrical regulations (e.g. PAT testing) and other national and international regulatory requirements.
    - Complies with the University of Aberdeen 'OS update and patching Policy'.
    - Where available, has up to date antivirus software operational.
    - Where available, has the device firewall switched on and configured in accordance with the guidelines issued by IT Services.
    - Has a 'Responsible Person', charged with ensuring the device and its use adheres to this policy and other applicable University of Aberdeen policies.

Network Specific Policies

Campus Network

The Campus Network is provided to support the teaching, research and administrative functions of the University by facilitating network connectivity to the University IT resources and to the Internet through JANET. It is the standard network to which most **University owned cabled devices** are normally connected.

Who

- Only staff authorised by the Director of IT Services are permitted to enliven ports on the campus network.
- Only staff authorised by the Director of IT Services and Responsible Persons are permitted to connect suitably configured devices to any Campus Network port.

- Only staff authorised by the Director of IT Services and Responsible Persons may configure devices for connection to the campus network.

What

- Only University owned devices may be connected to the campus network. Such devices must be configured for the particular location where they are to be used.
- In exceptional circumstances non University of Aberdeen equipment may be connected to the campus network (**Note:** eduroam is usually more appropriate for such devices). In such cases the device owner will be held liable by the University of Aberdeen for any loss arising out of the use of the device on University of Aberdeen networks and must consent to:
    - The University of Aberdeen monitoring the device activity.
    - Provide full access to the device if required to undertake investigations.

eduroam

The eduroam Network is provided to support the teaching, research and administrative functions of the University by facilitating network connectivity to the University IT resources and to the Internet through JANET. It is the standard network to which most **non University owned devices** and **Wireless devices** are normally connected.

Who

- Only staff authorised by the Director of IT Services are permitted to configure the eduroam network.
- Any registered user of University of Aberdeen IT services or registered user of an 'eduroam federated' organisation may connect a client device to the eduroam network.
- The University of Aberdeen does not specify who may configure **non University owned devices**.

What

- Any client device may be connected to eduroam network.
- University of Aberdeen users are required to ensure that devices are fully patched, have up-to-date, antivirus software and personal firewall installed, where possible.
- Non University of Aberdeen users are recommended to ensure that devices are fully patched, have up-to-date, antivirus software and personal firewall installed.
- The University of Aberdeen will not be responsible for any loss arising from connecting devices to the eduroam Network.

UoA-Gaming

The UoA-Gaming Network UoA-Gaming is a wireless service that allows any device that is incapable of using 802.1x authentication (e.g. Playstation, Apple TV, etc.) to connect to a network service. This service does not offer the same level of security as the eduroam wireless service. You should therefore only use UoA-Gaming for devices such as games consoles, Amazon Fire TVs and smart TVs. UoA-Gaming is available in all University of Aberdeen halls of residence. The UoA-Gaming Network is provided to support responsible social and recreational use.

Who

- Any registered user of University of Aberdeen IT services may connect a client device to the UoA-Gaming network, Note: not all categories of user are allowed to connect to this network.

- The University of Aberdeen does not specify who may configure **non University owned devices**.

What

- Any client device may be connected to the UoA-Gaming network.
- All users are required to ensure that devices are fully patched, have up-to-date, antivirus software and personal firewall installed where applicable.
- The use of a client device to connect personal electronic equipment, such as games consoles, is not regarded as configuring the network. Users so doing so should be aware that they will accountable for any use of devices connected in such a manner.
- The University of Aberdeen will not be responsible for any loss arising from connecting devices to the UoA-Gaming Network.

IT Classroom Network

The IT Classroom Network provides connectivity for the teaching classrooms, public access clusters and lecture theatre systems.

Who

- Only staff authorised by the Director of IT Services are permitted to configure the IT Classroom network.
- Only staff authorised by the Director of IT Services may connect devices to the IT classroom network.
- Only staff authorised by the Director of IT Services may configure devices on the IT classroom network.

What

- Only devices directly supporting the classroom or lecture theatre environment may be connected to the IT Classroom network.

Central Server Networks

Central Server networks are built to provide the necessary traffic management and security to effectively deliver the IT services connected to them.

For each server network a record will be kept detailing the purpose of the network, what connectivity it provides and the security measures to be implemented to protect the services connected to it.

Who

- Only staff authorised by the Director of IT Services are permitted to configure Central Server networks.
- Only staff authorised by the Director of IT Services may connect devices to the Central Server Networks.
- Only staff authorised by the Director of IT Services may configure devices on a Central Server network.

What

- Only devices consistent with the purpose of a specific server network may be connected to a specific server network.

Special Networks

There are devices, such as scientific equipment, which require a network connection but cannot meet the requirements of any of the above networks. In these circumstances, provided there is a business case, a special network may be configured. These networks

are subject to specific agreements between the device administrator(s) and IT Services. Only the minimum connectivity consistent with use of the device will be provided.

For each special network a record will be kept detailing the purpose of the network, what connectivity it provides, including who may use devices connected to it and who may connect devices to it and what devices may be connected.

Who

- Only staff authorised by the Director of IT Services are permitted to configure a specific special network.
- Only staff authorised by the Director of IT Services or persons detailed in the agreement may connect devices to the specific special network.
- Only staff authorised by the Director of IT Services or persons detailed in the agreement are permitted to configure devices for a specific special network.

What

- Only those devices detailed in the agreement may be connected to the specific special network.

5. Management

Monitoring

Traffic levels and resource utilisation will be appropriately monitored, with records kept for at least 1 year.

With the exception of staff authorised by the Director of IT Services, the following activities are a breach of this policy:

- Scanning or monitoring of any University of Aberdeen network.
- Operating any device in promiscuous mode.
- Installing software for the purposes of network monitoring or scanning.

The allocation of network addresses (IP addresses) shall be managed by IT Services. Addresses issued for use with a device must not be used with any other device. When a device is no longer connected to the network, the address issued to it will be reclaimed.

Excessive use

Any device that consumes excessive network resource (e.g. bandwidth) such that it impacts the legitimate operation of other network devices may be disconnected or have its access to resource limited. Such measures will only be taken to the extent necessary to ensure proper operation of the network. IT Services may employ Traffic Shaping to manage bandwidth ensuring critical applications are given priority.

6. Auditing

Management data as detailed in section 5 above will be used by IT Services to ensure compliance to this policy. Network scans and statistical analysis will be applied. Third parties may be engaged to periodically report on the state of network security in all University networks.

7. Enforcement

A breach of this policy shall be considered a breach of the University of Aberdeen *Conditions for using IT Facilities* and will be dealt with as provided in them.

In particular IT Services has the authority to refuse to provide a network service to or restrict the service provided to any device or user it believes has or will breach this policy. Disciplinary or legal proceeding may also be instigated.

8. Definitions

Monitoring	Collecting information relating to network traffic. This could include source and destination addresses, traffic levels and data types.
Scanning	Working through range of network addresses or ports attempting to connect to each in turn.
Promiscuous mode	A mode of operating a network port on a client device so that it will receive and process all network traffic including traffic not addressed to it.
OS	Operating System.
Cabled device	A device connected with a cable as opposed to a wireless connection.
Fully patched	All critical and security patches older than 2 months are applied.

Title	University of Aberdeen Network Connection Policy
Author/Creator	• Alastair Matthews, Network Infrastructure Manager, IT Services
Owner	• Christine Mackenzie, TaD Team Leader, IT Services • Alastair Matthews, Network Infrastructure Manager, IT Services • Approved by University of Aberdeen Advisory Group on Information Strategy AGIS)
Date published/approved	May 2012
Version	1. May 2000 2. June 2003 3. May 2012 4. September 2019
Review date	September 2022
Audience	Staff and students, contractors, public
Related	• Conditions for using IT Facilities • Information Security Policy • JANET Acceptable Use Policy (external)
Subject/Description	The purpose of this policy is to define what can be connected to the University's networks and the standards that must be adhered to by devices so connected.
Equality Impact Assessment	-
Section	IT Services
Theme	IT, network, connection, wireless, servers, workstations, laptops, PDAs, printers, MFDs, CCTV, scanners, video conferencing, classrooms, clusters, lecture theatres, bandwidth