**Network-Connection Policy**

1. **Purpose**

***<Company Name>*** is responsible for the ownership, development, installation, operation and maintenance of the data communications network. With this responsibility comes the authority to take action necessary to safeguard the security of the network and minimize and contain potential risks to the ***<Company Name>*** and its employees, both operational and legal, from the consequences of network-related security violations and misuse. In this context, the purpose of this policy is to state clearly;

* ***<Company Name>’s*** responsibility and authority for the data communications network infrastructure
* ***<Company Name>’s***  responsibility for devices connected to that infrastructure
* End-users’ responsibilities in using such devices.

**2.0 Scope**

**2.1 To whom it applies**

This policy applies to all the employees, third-party employees and contractors of the ***<Company Name>***.

**2.2 What is covered**

The coverage of this policy includes:

1. The ***<Company Name>’s*** data communications network infrastructure; all devices connected to it and all external network connections.

2. Any and all devices utilizing the infrastructure, including those connecting via wireless & mobile technology

3. Protection and detection of threats against ***<Company Name>***’s systems

4. Threats from, but excluding risks to:

* Devices attempting to connect to the ***<Company Name>’s***  data communications network infrastructure that are not approved for network connection.
* Devices connected both to the ***<Company Name>’s*** data communications network infrastructure and to external network connections
* Networks that are not installed or approved by ***<Company Name>***

**2.3 Out of Scope**

This policy does not include guidance on the following aspects as they are covered in specific support and maintenance contracts or ***<Company Name>*** procedures:

* External suppliers access to the organization’s network
* Data point activation

**3.0 Policy Statements**

**3.1 Users of the Network**

Only registered users (i.e. those holding valid usernames and passwords) or those given permission by the administrator (or nominated deputy) are permitted to connect to the ***<Company Name>’s*** data communications network.

**3.2 Modifiers of the Network**

Only relevant ***<Company Name>’s*** employees and contractors are permitted to change, modify or otherwise configure any part of the data communications network.

**3.3 Network Devices**

Only relevant ***<Company Name>*** employees and contractors are permitted to change, modify or otherwise configure & connect network devices to the organization’s data communications network. All such devices will be solely managed & maintained by ***<Company Name>.***

**3.4 Client Devices**

**3.4.1 Organization owned or managed client devices**

If the client device is owned (or leased) and managed by the ***<Company Name>***, network connectivity is achieved by either plugging this equipment directly into an activated data point on the organization’s network or via the centrally provided wireless network.

**3.4.2 Personally owned client devices**

Users wishing to connect their personally owned client devices to the ***<Company Name>*** data communications network may do so only by using one of the following methods:

* Connect via the centrally provided wireless network.
* Connect via the clean access service.
* Connect (from outside the organization) via the Internet to those services explicitly provided by ***<Company Name>*** for personal use.

Any other method of connection is prohibited unless a prior written authorization is not obtained from the ***<Company Name>’s*** administration. It is the responsibility of the user of any personally owned equipment connected to the network to ensure that the equipment has the latest level of anti-virus software and security patches installed, and that these are kept up to date at all times.

**3.5 Non-client Devices**

Non-client devices may only be connected to the ***<Company Name>’s*** data communications network if prior written authorization has been obtained. Users wishing to connect this type of device must complete a server registration form and submit this to ***<Company Name>’s*** service desk. ***<Company Name>*** reserves the right to deny this type of request.

**3.6 Use of the Network**

The company’s data communications network may only be used for purposes defined in the ICT Acceptable Use Policy (AUP) and for no other purpose.

**3.7 <*Company Name*> Responsibilities**

***<Company Name>*** is responsible for:

* Managing the risks from any device connected to the network and implementing any necessary security measures to protect the network (and other linked networks)
* Managing the provision of IP addresses; protection via the network security infrastructure; user registration; authorization and authentication; and data point activation.
* Installing, connecting and managing networking equipment within the company’s data communications network e.g. switches, routers and wireless equipment.
* Monitoring and managing the ***<Company Name>’s*** data communications network for performance issues, abnormal loading, port and IP scanning, and other security threats.

**4.0 Policy enforcement and sanctions**

Any suspected breaches of this policy will be investigated under the terms of the ICT AUP.

**Source:** <http://www.salford.ac.uk/__data/assets/pdf_file/0005/516542/Network-Security-and-Connection-Policy.pdf>