Information Services
Regulations for the Provision of Network Services
on the University of Kent Network

1. Scope

1.1. These Regulations apply to the provision of network services on University owned and non University owned computerised and mobile equipment and devices directly connected to the University network.

1.2. In particular, these Regulations apply to wireless networking within a University campus; virtual private networking (VPN) or dial-up technologies to access to University IT systems.

2. Definitions

2.1. The network is the entire University data network at all campuses and centres.

2.2. Roles are defined in The University of Kent Information Technology Security Policy.

3. Connection of Equipment

3.1. In accordance with The University of Kent Information Technology Security Policy:

3.1.1. No equipment may be connected to the network without the prior permission of the Network Controller.

3.1.2. Any equipment connected to the network must be electrically safe in accordance with University Health and Safety Policy and manufacturers' recommendations.

3.2. The Network Controller may require the disconnection of equipment if:

3.2.1. It is a security threat.

3.2.2. It is likely to adversely affect the performance of other authorised activity on the network.

3.2.3. It is not being operated within the terms of The University of Kent Information Technology Security Policy.

4. System Administration

4.1. The system must be actively managed in line with the Security Procedures for Systems Administrators which covers:

4.1.1. The collection and use of information;
4.1.2. The actions to be taken when investigating suspected misuse/abuse;

4.1.3. Withdrawal of facilities;

4.1.4.Retention of data.

4.2. Suspected misuse/abuse of a computer system must be reported to the Investigating Officer via the IS Helpdesk.

5. Wireless Networking

5.1. Since wireless signals do not respect departmental or building boundaries:

5.1.1. The use of any wireless networking equipment on University property must be registered with the Network Controller with the exception of equipment used to access the University wireless network as a client;

5.1.2. In the event of conflicts, the Network Controller may withdraw permission to operate wireless equipment.

5.2. Wireless networking systems must allow only authorised users access to University computing facilities.

6. Virtual Private Networking

6.1. VPN gateways must be registered with the Network Controller.

6.2. VPN gateways must restrict access only to authenticated users.

6.3. VPN gateways should maintain sufficient records to allow investigation of computer misuse/abuse as detailed in the Security Procedures for Systems Administrators.

6.4. Users of VPN services must take all reasonable steps to ensure that the personal computer/mobile device or other computing equipment used to connect is operated securely and is free from virus infection.