REMOTE ACCESS TO UNIVERSITY PROVIDED SYSTEMS AND SERVICES POLICY

Remote Access to University provided Information Systems and Services

Overarching Principle

It is the policy of the University of Strathclyde that as far as possible all systems and services should be available to authorised staff and students on or off campus wherever possible.

Exceptions

- Where a new service is implemented and its project board decides that there are security implications with allowing off campus access.
- There are licensing restrictions limiting access to on campus use only.
- There are physical restrictions limiting access to a particular service.

Provision of Advice

Help and advice on accessing systems and services off campus is available at:

- http://www.strath.ac.uk/ithelpdesk/helptopics/remoteaccess/

Availability of Commercial Software

In addition to the services provided directly by the University, the University attempts to make available off campus, where possible, a wide variety of commercial software for downloading. This can be done via the PEGASUS Portal:

- http://pegasus.strath.ac.uk/

Responsibilities of Individuals

Individuals accessing services remotely must comply with all relevant University policies and regulations including:

- University Policy on Use of Computing Facilities and Resources
- Protection of Information held on Mobile Devices and Encryption Policy
- Anti-Virus Policy

In addition individuals must exercise due care and attention when remotely accessing services. The University of Strathclyde can take no responsibility for end user devices and networks that it does not manage. Poorly maintained or configured equipment outside of the University can represent a significant risk both to personal and University Information Security. Particular care should be taken when travelling and using equipment of unknown providence.

End user devices used to access University services:

- Must have appropriate anti-virus protection, firewalls, and be regularly updated with Operating System and application software security patches.
- Must not be used for any purpose that would be at odds with the University Policy on Use of Computing Facilities and Resources.

Networks used to access University services should have:

- Appropriate security enabled.

Information belonging to the University should be stored appropriately and encrypted where necessary.

Remote Access for External IT Suppliers

This is covered by the separate policy:

- Policy and Procedure for Providing Suppliers with Remote Access to IT Systems and Services