Document Control

Document Title:	**Secure Remote Access/Home Working Service Policy**
Document originator(s):	**David Bunting**
Date:	**11 December 2008**
Next review date:	**December 2009**

Version	Date	Author(s)	Notes on Revisions
0.1	08/12/08	D. G. Bunting	Initial draft
0.2	11/12/08	Project Team	Reviewed and amended
0.3	09/01/09	C. J. Jarvis	Reviewed and amended
0.4	13/02/09	D. G. Bunting	Updated with M. Walton's comments
1.0	16/03/09	D.G. Bunting	Updated with S. Vinall's comments

Academic Services

Secure Remote Access/Home working Policy

Introduction

The Secure Remote Access Home Working policy covers the Desktop Anywhere service, this service aims to provide authorised University personnel with a secure desktop session on a server located in the data centre. To ensure the security and maximise performance of the service for customers the following policy has been developed.

Secure remote access/home working Policy

1. Service Details

1.1. Overview of Service

1.1.1. The remote access service will provide applications compatible with Microsoft Windows XP and above.
1.1.2. Citrix Xenapp 5.0 will be used to deliver the remote access service.
1.1.3. Customers will not be allowed to install applications. Applications must be requested via the Help Desk (see point 1.2).
1.1.4. Active Directory will be used as the authentication mechanism for the remote access service.
1.1.5. The remote access service will allow customers access to their Active Directory U and N drives.
1.1.6. A Terminal Services roaming profile will be used to retain a customer's settings between sessions.
1.1.7. Customers will be automatically logged off the remote access system after 30 minutes of inactivity. This inactivity timeout will be subject to periodic review.
1.1.8. A customer's remote network connection must be at least 512KB Broadband or above; anything else will not be supported.
1.1.9. Versions of Windows subsequent to Windows Vista will only be supported on the remote access/home working service when supported by Academic Services.

1.2. Applications

1.2.1. Customers must submit a service request for new applications to be added to the remote access service. The business case and technical feasibility for this change will be assessed by Information and

Computing Systems (ICS) within Academic Services for suitability on the service.

1.2.2. Customers will be able to run **not more than two** instances of each application. Certain applications with a very large overhead may be subject to further restrictions

1.3. Security

1.3.1. Connections to the remote access service from outside of the University will be made through the SSL VPN (Secure Sockets Layer Virtual Private Network) ensuring a secure encrypted session.

1.3.2. Customers will be subject to the terms of the University's network security policy at all times.

2. Support

2.1. Overview of Support

2.1.1. Operation of the remote access software is supported on University-owned computers running Microsoft Windows XP and above. Provision of this support will be subject to the agreements that Schools and Services have made with Academic Services for delivery of IT support.

2.1.2. All support requests should be logged with the Academic Services Help Desk.

2.2. Support Limitations

2.2.1. Support for customer-owned computers is limited to the provision of documentation and advice on how to install the remote access client software.

2.2.2. ICS will not support a customer's home networking or broadband.

2.2.3. ICS cannot guarantee the speed of connection apart from when it passes over the University's network.

2.2.4. ICS will endeavour to ensure a customer's printer works from home but this may not always be possible and support will depend on the type of printer (awaiting confirmation from Academic Service home working task and finish group).

2.2.5. Access via Linux and Mac workstations is not supported.

3. Usage Charges

3.1. Academic Services is not responsible for any service charges relating to the use of the remote access service (e.g. Broadband connection subscription).

4. Information Security

4.1. Customers are responsible for ensuring all University data accessed remotely is kept secure and confidential.
4.2. Customers are responsible for ensuring that they comply with the University's information security policy at all times.

5. Rules and Regulations

5.1. The remote access service is subject to the University's guidelines covering home working.