Home Working Guidance

Security responsibilities - Working from home

Purpose of document

To outline the security responsibilities, risks and the measures to be taken when members of the University, or other users of University Information Services, are working from home.
This is in addition to any other legal, contractual etc. requirements that may apply to this activity.

Relevant policy references

This guidance is to support the requirements of the following policies and regulations of the University

- Regulations for the use of computers, voice, data and the internet
- Information policy
- Data protection policy
- Information Access and Security policy
- Home working policy

Scope of activities

Working from home includes the following activity areas:

Activity Area	Activity
Information Handling	• Handling University data on removable storage (devices and laptops)
Use of Services	• Remote access to University services

Systems	• Managing
	  ○ Personal computers
	  ○ University supplied computers

Main User Responsibilities

These are defined in the University policies and regulations

- Prevention of unauthorised access to University information and resources
- Making proper use of University resources
- Prevent misuse of or overload of University services
- Reporting misuse of services or loss of University information

Use of University facilities at home is for your own work-related use, and is provided only for properly authorised purposes. You have a responsibility to ensure that other people do not have access to the University's facilities and services, or any confidential University information, and that you do not use the University's' services for personal purposes. You also need to protect the University's' services from threats such as viruses when connecting remotely. Any loss of confidential University information in your care, or misuse of the services you have access to should be reported as soon as you become aware of it.

Measures to ensure information safety when working from home

- Remote access to restricted (internal) University services should only be accessed via Virtual Private Network connection. This does not apply to services designed to be accessed via the internet (SUSSED for example).
    - A VPN connection must not be used for non-university use

        - Disconnect when not in use
        - Any use while connected to the VPN is subject to University regulations
- All software on any computer used to access internal University services should be kept up to date to prevent viruses
    - Automatic updates of software should be enabled
    - On personally owned computers, a software scanner should be run to identify out of date software
- An up to date virus checker must be installed and running
    - The updates to the software and the virus signatures must be turned on and working
    - The machine should be scanned regularly for viruses
    - If a virus has been found, the machine should not be used to access the University (or any other sites requiring valuable data or logins) until the machine is secured and free from viruses
- Any University data taken 'off site' shall be protected against unauthorised access by any third party. Security measures appropriate to the classification of the data must be implemented
    - Data must not be stored where other users of the computer may access it
        - If possible data should be kept on University filestore or in university applications and accessed remotely
        - Access to any local copies should be controlled by additional passwords or encryption, or kept in folders only accessible to the authorised user
    - This applies to data on the hard disk and stored on any removable devices
- You must not provide any other person access to University IT services
    - Do not ever allow applications to store login passwords for automatic login in future
    - Lock the computer when away from the machine

Key Risks addressed

- Information used or accessed away from the University may be accessed by unauthorised persons if they gain access to computers and other storage devices
- Services may be accessed and abused by unauthorised parties making use of the computers, or by theft of usernames and password used to access the services
- University services may be used for unauthorised purposes, preventing their proper use and damaging the reputation of the University

Document information
Version 0.2 Draft
Author Brevan Miles
Date 28/04/09
Safe Information Practices guidance