

Working at home: Freedom of Information, Data Protection and Records Management implications.

This guidance is intended for all Faculty of Sciences staff and researchers that work at home, either on an occasional or a regular basis. It applies to anyone undertaking administrative, research or teaching-related work at home.

This guidance gives general advice on the issues you need to consider ensuring that any University information you work on at home is protected from loss or unauthorised access and exploitation, while also ensuring that it is accessible to anyone that needs to use it for their work. It applies to information in all formats, including paper files, electronic data, word processed documents and e-mails.

The Data Protection Act 1998 and the Freedom of Information Act 2000 apply to all information that you receive and create as part of your employment or research with the University, regardless of where you work or store that information.

The Data Protection Act permits people to see information that the University holds about them while the Freedom of information Act will give people the right (from 1st January 2005) to access any other recorded information that the University holds. The Data Protection Act also requires us to hold information about living identifiable individuals for no longer than is necessary, to ensure that information is accurate, and to adopt appropriate security measures for this information to protect it from unauthorised access, amendment or deletion.

The primary copy of University information should not be stored at home, so University records should be updated as soon as possible with copies of any work that you do at home. This applies to all research, teaching or administrative work. This allows anyone who needs to refer to the records in your absence to be able to access the most up-to-date information. It will also ensure there is a back up copy of the work, if you were to lose your work at home. Finally it will enable the University to respond to any Freedom of Information or Data Protection request for that information without having to ask you to search information you have at home.

You will need to take reasonable measures to protect the information from unauthorised loss, access or amendment whilst stored at home. This will enable the University to comply with our Data Protection Act obligations and is also in the University's business interests: depending on the nature of the information involved, if someone inappropriately gained unauthorised access to University information it could cause reputational, commercial or competitive damage to the University. For example sensitive information about students or staff, or the exploitation of another person's research work.

If you can do so, it is recommended that you use a broadband connection to work directly from/to the appropriate University server via 'my portal' this will remove the need to take home electronic information or to store it there (IS can provide you with further information about this facility contact or email 3800). Using it will mean that when you work at home

you probably will not need to take any measures with regard to electronic information and your principal concern will be to protect your paper information.

The paper information you use at home is most vulnerable to loss or unauthorised access in the following ways:

- As a result of leaving papers in household areas where they may be seen by other members of your household or by visitors. This is most likely to cause difficulties when the information is about identifiable individuals.
- As a result of crime e.g. theft
- As a result of loss, particularly on the journey to and from work

All paper information must be held securely within the home environment.

Unless you work directly from/to the appropriate University server via 'my portal' the electronic information you work on at home is vulnerable to loss or unauthorised access or amendment in two ways:

- Physically, through the loss, damage or access to the computer or storage medium on which the record is held, most commonly loss of flash drives or unprotected security access on home computers. (One option might be to create an account on this PC, use it exclusively for work and password protect the account so that accidental access by other household members is avoided)
- Remotely, through someone accessing (hacking) your computer while it is connected to the Internet or through a virus. Kaspersky anti-virus software can be downloaded for your home computer from the uni. website <http://www.staffs.ac.uk/antivirus>. (Always ensure your computer systems and applications are up to date with security patches – Windows users can use the Windows update site to help with this. Always use a firewall, Windows firewall is sufficient but enhanced protection may be provided by your internet service provider, be available as part of the router or through installation of a personal firewall package). To ensure Windows Firewall is enabled go to Control Panel and Windows Firewall. Similarly if you are on a Mac you can check the firewall is enabled by going to System Preferences, Security, Firewall.

When deciding what reasonable security precautions you need to take against these vulnerabilities, it is necessary to balance their financial cost, time and practical implications against the seriousness of the damage that would result if someone did see the information or made unauthorised alterations to it. Depending on the nature of the information this damage could entail **legal action against you or the University, damage to your research or that of your colleagues, co-authors or fellow grant applicants, damage to the University's or your reputation; or damage to collaborative relationships caused by the inappropriate release of information.**

If you have used your home PC to work on sensitive University information or information about living, identifiable individuals (such as raw research data), when you dispose of the

computer you must make arrangements to ensure that the sensitive information is no longer accessible.

You should not store the official record copy of University information on a laptop that is regularly away from the office as the information is not readily accessible and is vulnerable to loss or theft. If necessity requires that the official record has to be stored on a laptop, you should make arrangements to back up that information so this it is not lost in the event of failure, theft or loss. You should ensure that appropriate security measures are taken to prevent unauthorised access to information.

Finally, you should never use a non- University e-mail accounts for University business. All University e-mail accounts are accessible via the internet.

A.Jones (12.7.2010)