

Working at home: records management and freedom of information implications

For whom is this guidance intended?

This guidance is intended for all University staff 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.

What is the purpose of this guidance?

This guidance gives general advice on the issues you need to consider to ensure that any University information you work on at home is protected from loss or unauthorised access and exploitation, while at the same time 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.

Addressing these issues will also help you to comply with the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002.

Why do freedom of information and data protection affect me when I work from home?

The Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002 apply to all the paper and electronic information that you receive and create as part of your employment 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 (Scotland) Act gives people the right 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.

We have 40 calendar days to respond to a data protection request and 20 working days for freedom of information request. These deadlines mean that the University must know what information it holds, and must be able to retrieve that information even if key staff are away. The Freedom of Information (Scotland) Act even includes a statutory code of practice on records management which describes the systems we should have in place for managing our information so that we can do this.

How does this affect how I work at home?

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 that you do at home. This means that anyone who needs to refer to the records in your absence will be able to access the most up-to-date information. It will also ensure that there is a back up copy of the work you have done so that, even if your home PC breaks down, you will not lose your work. If you require further guidance on back ups, please contact your IT support service. Finally it will

enable the University to respond to any freedom of information or data protection requests for that information without having to ask you to search information you have at home.

You also need to take reasonable measures to protect the information you take home from unauthorised loss, access or amendment. This will enable us 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 inappropriate gained unauthorised access to University information it could cause reputational, commercial or competitive damage to the University. For example, sensitive information about members of staff might be disclosed inappropriately, causing them distress, or someone might try to exploit 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 a Virtual Private Network as this will remove the need to take home electronic information or to store it there. Your IT support service can provide you with further information about this facility. 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.

Those parts of the University that receive IT support from MIS can also use a dial in connection to access electronic University information. Provided that you do not download copies of this information to your personally owned computer, this facility will also reduce the measures you need to take to protect the electronic information you work on. However, working in this way is likely to be expensive as it would require continuous use of the telephone while you are working. Regular users of the dial in service may find it more economic to install a Broadband connection instead.

How do I decide what security measures I need to take for information I use at home?

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 of a briefcase.
- As a result of loss, particularly on the journey to and from work.

Unless you work directly from/to the appropriate University server via a Virtual Private Network, 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. This is most likely to happen on the journey to and from work, or as a result of a theft from your home. However, a member of your household might also access information accidentally, for example, if information is stored on a household PC without further protection.
- Remotely, through someone accessing your computer while it is connected to the Internet or through a virus. If you use a broadband connection, whenever your

computer is switched on and not only when in use, it is possible for someone to access your computer.

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 to 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.

For information that is in the public domain or that we would release in its entirety if we were asked for it under a freedom of information request, the risks are low, and so little or no security measures are required. For information of low sensitivity about living identifiable individuals, such as a person's non-degree essay marks, slightly more security measures are required, mostly to protect against theft of the physical storage medium or accidental access by a household member. Sensitive information, whether about identifiable individuals or information that would affect the University's or another party's business or research interests, will require a higher level of security precautions. Examples might include research information about people's sexual life, unpublished research information, patent applications or information that connects named individuals with 'controversial' research topics (such as animal experiments or genetic modifications). For some information the risks may be so high that it should never be taken home. This might include medical information about identifiable patients (where a strong duty of confidentiality applies), or information whose disclosure is forbidden by law.

Thus there is a risk assessment involved in deciding what measures are required. These considerations can be represented in the following matrix:

	High	Medium	Low	Very low
How serious would the consequences be if someone gained unauthorised access to this information?				
How likely is it that someone could gain access to this information?				
What is the cost of the security precautions?				

The matrix will not provide you with a simple answer but is intended to help you to consider the issues involved. For example, if the consequences of someone gaining unauthorised access to the information would be very low, then you may decide that only low-cost security measures are appropriate. However, if the consequences of someone gaining unauthorised access to the information are high, and the cost of taking appropriate security precautions are also high, then you may decide not to work on that information at home. On the other hand, if the information is highly sensitive, but the necessary security precautions are simple and inexpensive, then you may decide to take the necessary measures and work on that information at home.

The University Records Management Section can assist with the assessment of the risks associated with unauthorised access to information, while your IT support service can advise on security options for electronic information.

I sometimes take University information home to help me with my work: does this matter?

You should try to avoid taking home the official record version of any University information as this makes it inaccessible to anyone but you. There is also a risk that the information will be lost in transit, for example, by leaving paper files on public transport or the theft of a jacket leading to the loss of electronic data kept on a memory stick. If you have taken the official record version, it may not be possible to recover this information.

Instead, staff that use Broadband at home should, if possible, access the University copy of electronic information directly via a Virtual Private Network. If you cannot use this service, or if you are working from paper information, you should try to take home a copy rather than the original information, whether this is an electronic copy on a 'memory stick' or a photocopy of the papers concerned. You should update the 'official' University record the next time you are at work.

If you cannot avoid taking home the official record, ensure that your colleagues know that you have it at home. If your section has a tracking and monitoring system, then this should be updated to show the record's location.

Whether you use a copy or the original information, to prevent unauthorised access to the information, it is important to take appropriate security measures to ensure that the information is not lost or stolen while it is out of the office, including while it is in transit to your home.

What are the implications of using my privately owned PC for work purposes?

Whenever possible, you should ensure that copies of University information are not stored on your private PC, including in temporary directories. In many cases it will be possible to avoid local storage of information by working directly from/to the appropriate University server via a Virtual Private Network. Your IT support service can advise you on how to do this.

If you do hold copies of University information on your privately owned PC, by law you will still be expected to produce them in the event that their subject matter is relevant to a freedom of information or data protection request. It is, therefore, advisable to store an official copy of the information in an appropriate file in a University office or on a University computer; this will avoid disruption to your home life in the event that we do receive a request for the information.

If University information other than very low risk information is stored, even for a short time, on a PC you keep at home, whether personally owned or provided by the University, you should take measures to prevent accidental access by household members and unauthorised access by intruders. 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. This would not be possible on older Windows systems. Any measures

taken should be proportionate to the sensitivity of the information involved; for example, for information of a low sensitivity it may be enough to make use of standard word processing document password options to prevent against accidental access, while more sensitive information will require stronger measures.

You should also take proportionate measure to protect this sort of information from remote unauthorised access. Always make sure your computer system and applications are up to date with security patches. (Windows users can use the Windows update site to help with this). Be aware that a computer connected via Broadband (ADSL or Cable) is vulnerable to attack when it is connected and not only when it is in use. In general greater security is available when using a modem/router than when using a directly connected Broadband modem, especially if you use a router providing Network Address Translation. Always use a firewall, which may be provided by your Internet Service Provider or be available as part of the router. Failing either of these options, install a personal firewall package.

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. This might involve erasure of the data or, in very extreme cases (for example, research data on identifiable victims of sexual crime) destruction of the hard drive. You may also wish to take similar precautions if the computer was used for your research records so that other people cannot access that research data. The University Records Management Section can assist in taking decisions as to the level of risk involved, while your IT support service can advise on the technical measures required to achieve this.

I use a University laptop to work from home: do I need to take any special measures?

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 means that the official record has to be stored on a lap top, you should make arrangements to back up that information so that it is not lost in the event of failure, theft or loss of the lap top.

You should also ensure that appropriate security measures are taken to prevent unauthorised access to information in event that the laptop is stolen and to prevent accidental access by members of your household.

I sometimes send and receive work e-mails from a personal e-mail account. Does this matter?

It is strongly recommended that you avoid using a non-University e-mail account for University business. Most University e-mail accounts are accessible via the Internet so it should be rare that you need to use any other account. Your IT support service can advise on how to access your University e-mail account remotely if necessary.

If you do have to use a personal e-mail account for University business, the e-mails you create and receive should be sent or copied to your University e-mail account so that they can be added to the relevant University record. In all cases, delete copies of work e-mails from any privately-owned PC and personal e-mail account, otherwise you will be required by law

to produce them in the event that their subject matter is relevant to a freedom of information or data protection request.

What help is available?

The University Records Management Section provides advice, guidance and training on data protection, records management and freedom of information issues. We can be contacted at recordsmanagement@ed.ac.uk. You should contact your IT support service for advice on IT issues. Please note that for privately owned PCs they will be able to give only generic advice on security issues as the details are specific to individual set ups.

Susan Graham
June 2005