

Everyday Records Management Good Practice: Interim Guidance

For whom is this guidance intended?

This guidance is intended for all University staff who generate records, including e-mails, in their day-to-day work.

What is the purpose of this guidance?

It recommends some techniques that staff can use to manage these records pending the development of comprehensive records management systems and procedures in their area. The everyday records management checklist provides a summary of these recommendations.

What are records?

For the purposes of this guidance, records are recorded information in any form, including paper, e-mail and other documents in computer systems, created or received and maintained by the organisation and our staff in the conduct of our business. They are kept as evidence of our functions, activities and transactions. These records are the basis for organisational accountability, compliance with legislative requirements and the development of the corporate memory.

Why do we need records management?

Information is a corporate asset. The University's records are important sources of administrative, evidential and historical information. They are vital to the University in its current and future operations (including meeting legislative requirements), for the purposes of accountability, and for an awareness and understanding of its history and procedures. They form part of the "corporate memory" of the organisation.

The need to improve the University's records management has become clear from several legislative developments including the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002. The Data Protection Act permits people to see information that the University holds about them (including information in e-mails, on personal drives of computers, or on home computers if you work from home) if they make a subject access request. As of 1 January 2005 the Freedom of Information (Scotland) Act will give people the right to access any other recorded information that the University holds (again, including e-mails, information on personal or home computer drives or meeting minutes). In both cases the legislation lays down statutory periods within which the University must respond to these requests for information: 40 calendar days for data protection and 20 working days for freedom of information. 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.

However we are not seeking to improve its records management functions solely because of the impending legislation. Records management also offers organisational benefits, including:

- Better use of physical and server space

- Better use of staff time
- Improved control of valuable information resources
- Compliance with legislation and standards
- Reduced costs
- Better records transferred to the University Archive

The University believes that its internal management processes will be improved by increased internal availability of information.

Who is responsible for records management?

The University's records management framework states that all University staff who create, receive and use records have records management responsibilities. These can be summarised as a responsibility to create records, to capture them in recordkeeping systems and to destroy those records that are no longer needed. Heads of Colleges, Schools, other units and business functions within the University have overall responsibility for the management of records generated by their activities, that is, for ensuring that records controlled within their unit are managed in a way which meets the aims of the University's records management policies.

The University Secretary has a particular responsibility in ensuring that the University corporately meets its legal responsibilities, and internal and external governance and accountability requirements. Day-to-day responsibility for this is delegated to the University Records Manager.

What information should I keep as a record?

Exactly what records you keep on file will vary according to the work you do.

Reasons for keeping records include:

- a. We need the information to carry out our business
- b. There is a legal requirement to keep the information
- c. We need the information for financial purposes
- d. We will need the information to explain why we arrived at a particular decision
- e. We will need the information if our decision is challenged in court
- f. We will need the information to be publicly accountable for our policies and decisions
- g. We will need the information to help us deal with similar situations in the future
- h. We will need the information to defend our rights and responsibilities, or the rights and responsibilities of others
- i. The information has value for historical research purposes

How should I organise my records?

Organise your records into files of information relating to the same issue, responsibility or transaction. For most topics there should be a single lead file. This will be the file of the person or section who has the lead on the topic concerned, for example, a committee secretary's set of minutes and papers. Other members of staff may also have a file on the same subject that they keep only for so long as is needed for their personal reference, but you should ensure that the lead file gives the complete story of our handling of the issue. If the content of a record is

important, it should be added to the file on the subject and stored so that it will always be accessible to all relevant members of staff. Only when there are confidentiality issues involved would it be appropriate to keep a record in a personal drive or a personal e-mail box.

In what format should records be kept?

Records may be kept as paper files, or electronically in shared drives, databases, or document management systems. Sometimes you may keep records on a website, but if so, ensure that they are adequately protected from tampering.

If you are keeping important records in an electronic format only, then you should ensure that you are confident that they will be legally admissible. The Records Management Section can provide you with guidance on legal admissibility on request. If you have records with long-term research value held solely in electronic form you should follow the guidance available on digital preservation on the University Library's website (<http://www.lib.ed.ac.uk/digpres/>).

Sometimes files are microfilmed or microfiched, but this is rarely cost effective. The Records Management Section can give further advice on this if necessary.

Irrespective of the method chosen to keep the records, a standard set of records management principles and tools can be used to manage them. The more important of these include filing schemes and retention schedules. See the introduction to records management and the more detailed guidance on individual topics for further information about these.

How should I manage my electronic files and folders?

If you create a folder or document on a shared drive, website or on your personal drive, you should take responsibility for managing that folder or document. They should have file titles which are easily understood by all members of staff. Do not name them after yourself, as no-one else will know what they contain. Likewise, only use commonly understood abbreviations. The title should clearly indicate the version status, such as, draft 1, draft 4, final version etc.

When placing information on a website, unless there are reasons for restricting the circulation of the document, try to place it on a publicly available part of the website. Making information available in this way is in line with the spirit of freedom of information legislation, and will help to reduce the number of freedom of information requests the University receives, as people will be able to access the information without having to ask for it.

If you have personal information in your e-mail or personal drive, please ensure that you save this to a folder called 'personal'. It may be necessary for other University staff to access your drives; for example, in response to a subject access request. They would only look at those marked 'personal' or in a personal folder in an extreme situation, whereas they may well have to access undifferentiated e-mails to deal with a request for information.

On which drive should I save my electronic information?

Shared drives should be used for information to which your colleagues may need access. Do not password protect material unless your colleagues know the password so that the information can be accessed in your absence. Use your personal drive for only for information, which is genuinely confidential or personal. Do not use your computer hard drive (usually the c: drive) to store information as this drive is not backed up.

University websites should be used for making available non-sensitive information, which is needed across the University for reference purposes, although the web version should not be the master copy if it is vulnerable to tampering. Wherever possible, place website information on the externally available website as making information widely available will minimise the number of freedom of information requests the University is likely to receive.

What points should I bear in mind when managing my e-mails?

E-mails are as much an official communication as is a letter, memo or a fax. Your e-mails may be disclosed in response to a freedom of information or data protection request and in legal cases. Electronic messages can be legally binding; contracts can be set up via e-mail and we may be held liable for defamatory statements in e-mails. For these reasons, do not say things in e-mails that you would not say in other forms of written communication. See the guidance on creating records for further information on the issues to consider when writing an e-mail.

If an e-mail contains important information or an important decision, it should be added to the relevant file, either by printing the e-mail to paper or by saving it to the relevant folder on a shared drive. In Microsoft Outlook this can be done using the File-Save As option. To avoid saving multiple copies of the same e-mail, it is usually advisable to adopt the following guidance:

- When the e-mail has been sent by someone who has access to the same filing system as the recipient, the sender is responsible for filing the e-mail; otherwise the first recipient in the 'to' list should take responsibility for filing it.
- When dealing with long e-mail strings, provided that the string has not been edited and all the previous e-mails are part of the string, it is sufficient to keep the last e-mail in the string and to destroy the others.

Most e-mails are about ephemeral matters. It is a drain on University resources to store them on our system and to search them when we have to respond to a subject access request. Delete ephemeral or out-of-date e-mails as soon as they are no longer required; do not allow a backlog to accumulate as this becomes difficult to manage. Sent e-mails should also be deleted regularly. The most efficient ways of doing this include:

- sorting sent e-mails by date and deleting all those over a certain age
- sorting sent e-mails by addressee and deleting all those sent to certain individuals
- sorting sent e-mails by subject and deleting those relating to completed business

- sorting sent e-mails by size and deleting large e-mails that are no longer required.

Opening and deleting e-mails on a case-by-case basis is time consuming and unlikely to be cost effective.

Some e-mail systems save deleted items in a folder rather than actually deleting them. Microsoft Outlook is one system that does this. It is important to ensure that e-mails you meant to delete are actually deleted. In Outlook, you can do this by setting your deleted items folder to empty whenever you exit Outlook. To do this take the following steps:

- a. On the Tools menu, click Options, and then click the Other tab.
- b. Select the 'Empty the deleted items folder upon exiting' check box.

For how long should I keep information?

The University is subject to very few legal or regulatory obligations to keep records. For most records, the decision as to how long to keep them is a business decision based on how long the information will be needed for the conduct of day-to-day business, for precedent, or for accountability reasons. In the long-term, your business area will develop or adopt a retention schedule for your records to ensure that all staff are following a consistent approach. However, in the interim you may need to take retention decisions yourself. Pages 3-5 of the Records Management Section guidance on developing retention schedules describe how to go about taking these decisions while guidance on how to select records that may need to be kept permanently as archives is available at <http://www.lib.ed.ac.uk/resources/collections/specdivision/criteria.pdf>.

It is rarely cost effective to make retention decisions on an individual document basis. Instead, take decisions at the level of individual files or collections of records.

Does it make any difference if I sometimes work from home?

The Freedom of Information (Scotland) Act applies to all information that you create as part of your employment with the University, regardless of whether you work at home, in the office or in the laboratory. The primary copy of University information should not be stored at home, so University records should be updated with copies of the work that you do at home. If you are working with sensitive information, you should take precautions to prevent unauthorised access to that information, for example, by ensuring that a copy is not saved to your home computer, and by using a lockable briefcase.

Most of my information relates to my research: does any of this apply to me?

The University's obligations under the Freedom of Information (Scotland) Act apply to research information as well as administrative information. Although research information should be organised in the way that best supports your research methodology, please bear in mind that other members of your school may need to access the information in your absence to respond to a freedom of information 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 data-protection@ed.ac.uk.

Susan Graham
September 2005