Best Practice in Disposing of Records

For whom is this guidance intended?

This guidance is intended for all University staff that need to dispose of records, on an occasional or regular basis. It is likely to apply to almost all University staff, including anyone undertaking administrative, research or teaching-related work.

The guidance applies to *all* records, regardless of the medium in which they are held, including e-mail, spreadsheets, databases and paper files.

What is disposal?

Disposal of records is the appropriate destruction or transferral to the University Archive of records, once they have reached the end of their retention period. The retention period and decision on manner of disposal should be set out in your area's retention schedule. For guidance on developing a retention schedule, see (http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/Retention/Retention.htm).

There are two ways of disposing of records:

- Appropriate destruction of the records which no longer have value
- Transferral of the records with continuing value to the University Archive (see http://www.lib.ed.ac.uk/resources/collections/specdivision/criteria.pdf for advice on the types of records of interest to the University Archivist)

Why do we need to dispose of records?

The retention of unnecessary paper and electronic records consumes staff time, space and equipment. It also incurs liabilities in terms of the need to service information requests made under Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002. In addition, the Data Protection Act requires us to keep records for no longer than necessary; we can be sued for retaining unnecessary information if this causes damage to someone.

When should I dispose of records?

Records should be disposed of in line with their retention schedule. Please note that you should not destroy records subject to a current information request until 40 days after the request has been answered. If you need to check whether a record is subject to an information request, please contact your local freedom of information practitioner (see http://www.recordsmanagement.ed.ac.uk/internal/practitioners/PractitionersList.htm).

The Code of Practice on Records Management issued under the Freedom of Information (Scotland) Act 2002 says that we must keep a record of the

destruction of records. Annex A contains a template you can use to do this. Freedom of information practitioners should keep completed forms for at least 20years as part of their documentation of their records management practices and procedures. Do not record the disposal of ephemeral or transitory material (eg a draft document or an e-mail of short-term significance) and convenience copies (that is, copies made and kept for ease of reference).

How should I dispose of records?

How you destroy a record depends on how sensitive it is, and in what medium it is held. If sensitive material is not properly destroyed, unauthorised access to that material (whether intentionally or accidentally) remains possible, and this could cause reputational, commercial or competitive damage to the University and any individuals named in the record. Paper records could be found on rubbish tips, while specialists can retrieve data stored electronically from computers. For example, in 2000, details of Sir Paul McCartney's bank accounts were found on a computer that a bank had sold without fully erasing the data from the hard drive.

Before disposing of records, you should consider which of the following levels of sensitivity would apply to them:

- *Low* (for example, information in the public domain or information that we would release in its entirety in response to a freedom of information request)
- *Medium* (for example, student mark sheets, policy documents about a policy proposal that has not yet been agreed, research in progress)
- *High* (for example, medical information about identifiable individuals, information identifying involved in animal experiments, commercially exploitable research)

When choosing the category into which your records fall, it may be helpful to consider the consequences for the University or another party should an unauthorised person gain access to the "destroyed" record.

Choosing the appropriate destruction method contains an element of risk assessment. It is for individuals to assess the security implications of the material and to dispose of it accordingly, balancing the risk of the information falling into the wrong hands against the time and effort involved in disposal to arrive at a proportionate response to the risk. These issues can be summarised in the following matrix:

	High	**Medium**	**Low**
How serious would the consequences be if someone gained unauthorised access to this information?			
What are the cost and time implications of the disposal method?			

The matrix will not provide you with a simple answer but will help you to consider the issues involved.

How should I destroy paper records?

If the record does not contain sensitive material, it can be disposed of through normal waste procedures, for example, in a recycling bin.

Sensitive paper records may be shredded, incinerated, pulped or disposed of through the red confidential waste bags. The University has a contract with a private contractor to destroy confidential waste in these bags for a fee. For further information about the University's confidential waste disposal services, see the entry for confidential waste in the University's waste disposal and recycling guidance. (http://www.eso.ed.ac.uk/Waste/WhatToDoWithIt/index.shtm#Confidential). Bags containing confidential waste should be stored in a locked room as otherwise an unauthorised person may gain access to them.

If the material is particularly sensitive, it is advisable to shred locally, as then you can be sure that the record has been destroyed. Shredded paper may go in the normal waste, or, for a "belt and braces" approach, in the confidential waste. However, shredding may be onerous and time consuming when you have a substantial number of records. For most sensitive material, using the confidential waste bags should be sufficient.

How should I destroy electronic records?

As part of your everyday use of your computer, you will probably "destroy" electronic records by deleting them. This often involves two stages. Files deleted from a computer c: drive are often placed in a "recycle bin", and some e-mail programs store deleted items in a "deleted items" folder. You will need to empty these periodically. It is good practice, if your email software has the facility, to set up your deleted folder to empty on exit automatically.

However, this sort of deletion does not eradicate the data. If a file or e-mail is deleted, it remains on the disk in a hidden form, and, for information held on servers or shared drives, will be kept on a back up tape for a specified period. Likewise, reformatting a disk may leave hidden data on the disk. It is possible to retrieve information deleted in this way. When dealing with sensitive information, further measures are necessary to erase the data fully.

In the case of information held on servers or shared drives, this will be the responsibility of the relevant computer service. For example, if you use a University e-mail service, then this information will be stored on a central server, and you will need to take no action other than ensuring that all your "deleted items" folders have been emptied. Your computer service will make arrangements for the appropriate disposal of the server and the back up tapes in due course.

If you have saved information to a PC or Mac hard drive, floppy disk, CD or other storage medium, you must take measures to ensure that the information is fully deleted before disposing of the item. For portable media such as a disk or CD, the best way of destroying the information they contain is to destroy the items concerned. Floppy disks should be bent out of shape, broken, or cut into pieces. CDs should be broken, or you should score lines over them.

To "destroy" information held on a hard drive you have to "destroy" everything that is on the drive, including software. For this reason, it is advisable to carry out this sort of destruction only when you are ready to dispose of the computer, whether by handing it on within the University, donating it to an authorised organisation for reuse, or sending the computer for recycling. If you are not handing the computer on, but wanted to make sure you had destroyed something, you would have to save everything you wanted to keep from the hard drive to another format, carry out the "destruction", and then reinstate the system, software and records that you wanted to keep.

All computers must be disposed of in line with the University's policy on the reuse and recycling of computers and other electrical equipment (http://www.eso.ed.ac.uk/Waste/WhatToDoWithIt/index.shtm#IT%20Equipment). Staff in MIS supported areas should contact their local computing support or MIS Customer Services if they want to destroy information on a hard drive or to arrange to dispose of a computer.

EUCS have prepared a "decommissioning" application which must be used by any unit not supported by MIS that wishes to pass a computer outside the University, whether for reuse or recycling. This is available at http://pie.ucs.ed.ac.uk/pie-2.0/doc/Decommission.html. Follow the instructions given there to overwrite all sectors of the hard drive, making it impossible for any software or information to be recovered from the PC. The tool also enables a simple operating system to be mounted onto the PC/laptop.

If your computer has been used to process highly sensitive information, you may also need to use the decommissioning tool before passing on the computer within the University. Your IT support service can provide you with advice on how to do this and how to reinstall the software needed by the computer's next user. Staff in MIS supported areas should contact their local computing support or MIS Customer Services about this.

Staff also have access to an EUCS electronic archive and may store whatever they wish on this permanently. At present, the only way to remove information from this archive is by physically destroying the archive, so you should not store highly sensitive material here. This may change when EUCS moves to the storage area network.

I want to sell my work computer, or give it to a charity. What measures do I need to take?

Staff working in MIS-supported areas should not pass their computers to charity or sell them; instead they should make arrangements with MIS Customer Services for their disposal.

For EUCS-supported areas, if you are passing or selling on a computer or computer parts, ensure that all data and software is erased as described above.

How can I destroy audio and video tapes?

Audio and video tapes should be recorded over with silence, unless highly sensitive, in which case they should be physically destroyed.

Are these measures really necessary?

Failure to comply with the Freedom of Information (Scotland) Act and the Data Protection Act can have serious consequences. A university in England disposed of a computer that had been used to store research data about paedophiles and their victims. A subsequent owner retrieved the data from the computer. As a result of this, the victims of the crimes and their families suffered significant distress, the university received substantial adverse publicity (including a feature on *Newsnight*), the university was sued for a substantial sum, and there was a risk that researchers' access to sensitive material would be curtailed in future. More information on this case is available at http://news.bbc.co.uk/1/hi/uk/1519889.stm.

Although this is an extreme case, it demonstrates the need to exercise extreme care in the destruction of highly sensitive material.

What help is available?

The University Records Management Section provides advice, guidance and training on records management, data protection and freedom of information issues. Contact us at recordsmanagement@ed.ac.uk. Your IT support service can advise on the options for the destruction of electronic information.

Antonia Kearton & Susan Graham
December 2005

Annex A: Template for recording disposal of records

Disposal of Records				
Section:	**Name:**		**Date:**	
Title of Record:				
Format:				
Reason for disposal:				
Method of disposal: (tick relevant box)	Destruction		Transferred to archive	
If destroyed, method of destruction:				
Date of disposal:				
Authority:				
Not subject to current information request: (tick once checked)				