RECORDS MANAGEMENT GUIDANCE 12

Disposing of Information

THE UNIVERSITY *of York*

Disposing of Information

Why dispose of records?

- To save space, time and equipment.
- To find the right (version of) information quickly and efficiently.
- To meet obligations under the Data Protection and Freedom of Information Acts.
- To avoid attracting unnecessary liabilities by holding on to records for longer than they're needed, while ensuring that information which is really needed is retained.

What should I dispose of securely?

Information should always be disposed of safely and securely, however, the more sensitive the information, the greater the level of security required.

Secure destruction is especially important where the information contains personal or sensitive personal details, is confidential or is commercially/financially sensitive. The Data Protection Act legally requires us to ensure that all personal information is destroyed in a secure manner. Similar standards of security may also be imposed by contractual obligations, regulators or University policy.

Ordinary Waste/Disposal

- Information which could be released under a FOI request – e.g. information that's already publicly available or which wouldn't attract an exemption, cause harm, distress or embarrassment.

  - Mission statements
  - Regulations
  - Published directories
  - Internet websites
  - Published minutes
  - Press releases
  - Prospectuses
  - Presentation materials
  - Course guides and outlines
  - Publicity material
  - Published surveys
  - Magazines
  - Published circulars
  - Published reports

Secure Disposal

- Personal data (information which identifies people directly/indirectly and affects their privacy)
  - names & addresses

Secure Disposal
o exam scripts/student work o financial/payment/credit card details o job applications o interview notes o disciplinary records o emails
• Sensitive personal data o Information on someone’s health, race, ethnicity, beliefs, sexuality, offences, religion, political affiliation or trade union membership ▪ Sick pay, maternity pay records ▪ Accident books, health and safety records ▪ Personnel records ▪ Admissions records ▪ Student records ▪ Equal opportunities monitoring data ▪ Medical records ▪ Grant applications
• Information given in confidence o references o questionnaires and research data gathered under duty of confidence o medical information o advice from lawyers
• Commercially sensitive information e.g. information which, if disclosed might: cause financial loss or loss of earning potential; facilitate improper gain; give unfair advantage for individuals or companies or undermine someone’s ability to compete fairly. o tenders o contracts o purchasing records o unpublished accounting records o IPR records (unpublished research, draft manuscripts)
• Information which would disadvantage the University in commercial or policy negotiations with others.
• Information whose accidental disclosure might cause someone harm, distress or embarrassment
• Information which might compromise security / health or safety o systems’ documentation o passwords o security protocols

Secure Disposal
o building plans
• Reserved/closed/unpublished minutes and papers
• Information which does not yet form the settled view of the University o unapproved strategy documents
• Information where secure disposal is required by the terms of a contract/licence or by statute or its disclosure would breach a statutory restriction.

Disposal Methods

Transfer to the Archive

While most records at the end of their life will be disposed of by being destroyed, a small proportion will be transferred to the University Archive. These will be records which have an enduring value as evidence or an historical record (e.g. minutes of key committees, prospectuses and handbooks, photographs, regulations). More information on the Archive and its holdings can be found at www.york.ac.uk/recordsmanagement/archive.

Destruction

Paper – non confidential

Paper records that do not contain any personal or otherwise sensitive material (see above) can be disposed of in office or recycling bins. If you need a recycling bin in your area, or have a large amount of paper to be taken away then please contact Campus Services.

Paper/microfiche – confidential

Sensitive/confidential manual records should be disposed of as soon as possible after their retention period has elapsed and destroyed by secure means (e.g. cross-cut shredding or incinerating).

With sensitive and confidential material it is important to maintain levels of security throughout the record's life. It is no good keeping information on restricted drives or in locked filing cabinets only to leave the confidential waste bag in an insecure location. Levels of security must be maintained until the point at which the information is physically destroyed.

Further information on available mechanisms for secure disposal can be found at **http://www.york.ac.uk/campusservices/cleaning/waste/disposal/secure.html**.

Confidential waste bags are available from the Mail Room on request. Collection can be arranged by contacting admn203@york.ac.uk. For the disposal of microfilm contact Jill Thackrah in Campus Services.

If your department has a cross-cut shredder, this can be used to shred confidential papers. The shredded paper can then be collected for recycling. This allows for the most environmentally friendly means of disposal and reduces the cost to the department/ University of outsourced confidential destruction, while providing a suitably secure means of disposal.

Computing Equipment

Any machine or device (e.g. laptop, memory stick) that has been used to store personal data or sensitive information should be disposed of only after reasonable precautions have been taken to erase the data on it.

While important steps can be taken to limit the amount of information stored on the computer/device itself (by storing it more securely on maintained shared-drives and servers which will be backed-up and offer more security), you should remember that information may still exist on your hard drive (for instance in the form of temporary files, web caches and logs).

A computer's hard drive or any portable storage device (e.g. memory stick) should always be completely wiped before the hardware is sent for recycling or disposal. Where sensitive personal information has been stored on the computer, physical destruction of the hard drive should also be considered.

Particular advice on wiping drives and disposal methods for computing equipment should be sought from IT Services. Having wiped the hard drive, advice on arranging for the physical disposal of hardware is available from Campus Services. University-owned computers should NOT be disposed of at the tip.

Some projects, agreements and research contracts may specify disposal of digital data to a particular standard. Further advice and support is available from IT Services, who also maintain the University's policy on the disposal of servers.

Compact Discs, Videos, Identity cards etc

Where the information on a CD is neither sensitive nor confidential, having first been wiped/re-formatted, the CD can be sent for recycling to Campus Services.

Not all CDs can be wiped permanently (e.g. non-rewritable CDs). Where the information cannot be thoroughly wiped, or the information is of a particular sensitivity as to warrant secure physical destruction (in addition to the wiping), these CDs and identity cards can be destroyed as confidential waste by prior arrangement with Campus Services.

Video and audio tapes should be wiped by being recorded over with white noise before being disposed of. IT Services has a bulk eraser for backup and VHS tapes.

Contact Jill Thackrah in Campus Services, for information on arrangements for the physical destruction of discs, tapes and cards.

Back-ups and other copies

Backed–up and archived/recovery data will be subject to the same level of security as live data, therefore equal care should be taken with its disposal.

Information on centrally-maintained servers is regularly backed up and these back ups are routinely destroyed after a set period – normally 6 months. Destruction of this data is the responsibility of IT Services or the department maintaining the server.

As information held by the University, information stored as a back-up copy also falls under the auspices of the DPA and FOIA. It is of little use destroying one instance of a record if other instances still exist as backups on a CD and PC hard-drive, or as copies on a memory stick or laptop, and therefore in making the decision to dispose of information, this should be enacted consistently.

Avoid the proliferation of multiple copies of documents (whether in electronic or hard copy). Where this is unavoidable, make it clear which is the master copy, who is responsible for maintaining the official record and give the version number and date of the document. This will help ensure that the right information and instances are destroyed at the right time.

Keeping a record of what you destroy

Knowing what you don’t hold – and why – can be as important as knowing what you do hold. Keep a record of any significant destruction or transfers of records. This is important for a number of reasons.

- Operational efficiency (avoiding the need to hunt for material that isn’t there, not assuming data was destroyed/lost when it wasn’t, and having clear audit trails for our information).
- Defence against malicious disposal. Under Freedom of Information, it is an offence to destroy information that is subject to an active FOIA or DP request. A disposal record establishes that information was destroyed properly and justifiably, and not maliciously.
- Compliance. A disposal record also helps with audit exercises, legal discovery cases and defences, demonstrating good record quality, management and compliance. Disposal procedures should also be documented.

Remote working

Information created as part of your job is information that is held by the University. As such it should be handled in accordance with the University's regulations and policies and is liable to legislation such as the Data Protection Act and Freedom of Information Act. This remains the case if you take information home or access it remotely. Thus University information stored on USB sticks, laptops and home PCs will require the same standard of care and be subject to the same statutory, regulatory and institutional obligations, and same standards of security, as the University information held on central servers or in our offices.

The University's policies in relation to data security and the management, use, disclosure, and disposal of records should be applied to the information irrespective of whether it is held electronically or in paper format, in your office at work or home. Security should be proportionate to the sensitivity of the data and risks of the environment. Staff can be liable as individuals for the use/misuse of the information in their care, and any breach of the University's policies and regulations will be treated as a serious disciplinary offence.

Out-sourcing the storage and disposal of information

Where the information includes personal data that are being stored, destroyed, or otherwise processed, by a company or third party on the University's behalf, the University remains responsible for its care under the Data Protection Act and is obliged to have a contract in place with the organisation or individual. The contract should ensure an appropriate standard of care for the information, compliance with the Data Protection Act, and make clear where responsibilities and liabilities lie. The contract should specify the purposes for which the data is being given and ensure that any actions taken in respect of the information are only done with the University's prior, written authorisation. A model agreement has been drafted for use by departments and is available from the Supplies Office, Records Manager and IT Services. Actions and processes should be auditable, and further advice should be sought before entering into such contracts.

Making disposal easier: act at the point of creation

To ensure that the right information is destroyed, it is important that files are records are labelled clearly and carry the right information. Having clear and standard file-names, and making sure that records give details such as their date(s) and version number, their draft/final, official/duplicate status, all facilitate the correct and easy disposal of records. Similarly recording when a file is closed or due for destruction makes implementing disposal decisions much easier.

Are records filed in such a way as to enable their retention periods to be applied? For instance, can going through and weeding out certain documents within a file be helped by the way the file is organised (e.g. sub-sections)?

Specific requirements for the disposal of certain information

Research Sponsors
Contracts governing the provision of access to research data and the funding of research often specify how and where data are to be stored, accessed and disposed of. With funding council regulations, they may require material to be retained for a certain period, and core datasets to be transferred to, or deposited in, a recognised repository or archive and for material to be destroyed to a recognised or auditable standard. The standard for destruction may, in some cases, differ from or exceed that recommended in university guidance and therefore special attention should be paid to such obligations.

Credit Card Information
The retention and disposal of credit card details must conform to the Payment Card Industry Data Security Standard (PCI DSS). This industry standard came into force in June 2007 and relates to the storage and disposal of credit card information (including such information stored in databases, emails or in hard copy). A copy of the standard can be viewed at **https://www.pcisecuritystandards.org/**

Information from Criminal Record Checks
The Criminal Records Bureau (CRB) Disclosure service has a Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. **http://www.crb.homeoffice.gov.uk/guidance/rb_guidance/handling_of_disclosure_info.aspx** Registered Bodies should include retention and disposal procedures in their policies for the correct handling and safekeeping of certificate information.

Stories in the news

Not disposing of information thoroughly and safely can result in severe penalties and reputational damage, as some of these stories show:

- http://news.bbc.co.uk/1/hi/england/west_midlands/4288409.stm
- http://news.bbc.co.uk/1/hi/wales/wales_politics/7509151.stm
- http://news.bbc.co.uk/1/hi/programmes/breakfast/4271485.stm
- http://news.bbc.co.uk/1/hi/uk/7602402.stm
- http://www.bbc.co.uk/devon/news/032002/07/confidential_files.shtml
- http://news.bbc.co.uk/1/hi/england/dorset/4625434.stm
- http://news.bbc.co.uk/1/hi/uk_politics/8354655.stm