UNIVERSITY OF LIVERPOOL | COMPUTING SERVICES

Records Management Guidance: Electronic Records Management (ERM)

What are electronic records and why is good ERM important?

An electronic record is 'a record that is created, generated, sent, communicated, received, or stored by electronic means and that requires some form of computer technology to access and use.'[1]

Although electronic records do not have the same physical presence as paper records, it is still very important to manage them efficiently. The Records Management policy, together with the Retention Schedule, and the general guidance on our website applies to both paper and electronic records.

Electronic records are particularly at risk of data loss, unauthorised access, duplication of work, and failure to comply with legislation. Poor ERM is linked with wasted time and storage space (physical and electronic), an *ad hoc,* uncoordinated approach across the University, and possible negative publicity.

Beginning ERM

ERM needs to start at the point of creation. There are a number of options about what system you use to create the record (e.g. word or email), where you store it (e.g. shared drive, personal drive, CD), and how you share it (e.g. VOCAL, email attachment, printout). You will make better decisions on all of these aspects if you think carefully about why you need the record, who needs access to it, what controls there need to be on access, and how long it needs to be kept for. Refer to the Summary of Storage Locations Table on page 3 below for help with these decisions.

Good practice in ERM

- *Filing*: Consider setting up a shared central filing system for both paper and electronic records. For further information see the Guidance Note on Filing and File Naming.

[1] International Records Management Trust

- *Access & Security*: Carefully balance the requirements for staff access to records against security needs for confidential or sensitive information. Be aware of University policies on Information Security, Data Protection and Freedom of Information. Consult the guidance produced by CSD when using mobile devices.

- *Sharing Documents*
  - If using SharePoint to collaborate on work in progress then ensure the final version is filed appropriately at the end of the project. For further information see also the Guidance Note on Version Control.
  - Documents created in Microsoft Office might contain information that you would not wish to share publicly such as hidden data or tracked changes, so it is a good idea to remove this before sharing an electronic copy with clients or colleagues. You can do this using the Document Inspector feature.
  - If you need to encrypt individual files and folders to protect data rather than complete devices, follow Computing Services guidance on using Bitlocker or AXCrypt.

- *Metadata/ Document Properties*: Metadata is 'data about data' i.e. information about your records. In Microsoft Office, this is referred to as 'Document Properties'. It includes details about a file that help to describe, identify or retrieve it, such as title, author name, subject, and keywords. It also helps other users to understand how electronic record keeping systems were set up and how they should be used. Metadata can also be tailored to record things such as the retention period. Guidance on using this feature is available on the Microsoft website.

- *Legal Admissibility*: For digital records to be legally admissible, they need to be proved to be authentic and accurate. If your records are considered the primary legal copies, you should aim to comply with the British Standard BS 10008:2008, *Evidential weight and legal admissibility of electronic information*, and BIP 0008:2008, *Code of Practice for the implementation of BS 10008*.[2] For guidance please contact Legal Services.

Special Projects involving Electronic Records

- *Scanning*: If you are scanning paper records to keep the electronic copies as part of the electronic filing system, make sure that they meet requirements for legal admissibility if necessary (see above).

- *Web Pages*: Save and file the documents used to create web pages, so that information can be quickly recovered if it is accidently deleted or lost from the web drive, and so that there is evidence of former versions of the pages in case of any query.

- *Legacy Electronic Records*: These are old records that do not fit into current filing systems. They may be on a shared or personal drive, but could also be stored on tape, CD, optical drive, floppy disk or other device. For advice on dealing with these, please see the Guidance Note on Legacy Records.

[2] You can access the British Standards Online database through the electronic library. http://atoz.ebsco.com.ezproxy.liv.ac.uk/Customization/Tab/11404?tabId=8817

Preservation

Electronic records are vulnerable to deterioration over time. It is vital to ensure that the data contained in electronic records retains its accuracy, authenticity and readability, throughout the record lifetime. For electronic records that are going to be needed for 10 years or more, please contact CSD to ensure that they will be able to support the readability. This is particularly important if you hold electronic records that are in an unusual format, as the originating application may no longer be available. Also, avoid storing such records on equipment such as CDs, DVDs and USB pens as the data can easily become corrupted. Convert documents to .pdf format where possible, as this format is relatively stable and readable.

Destruction

- Review all records regularly, and delete items which are no longer needed.
- You may use the RM Confidential Waste Destruction Service to dispose of information on CDs, DVDs, or USB pens, so long as you make it clear that it is non-paper waste.
- Use the CSD Disposal Service for redundant IT equipment.

Useful Contacts

Records Management for advice, guidance and training on all aspects of records management.
Legal Services for advice on legal admissibility, data protection and freedom of information.
Computing Services for advice on IT issues, such as software and hardware requirements.
Special Collections & Archives for advice on historical/ research value and formats for long-term digital preservation.

Future Developments

Records Management is working on these issues with Computing Services, Legal, Risk and Compliance and other key players. The Records Manager can advise departments on electronic records management.

Summary of Storage Locations Table

Storage type	Use for	Explanation
Laptop	Working away from the office, but not to store records. Data should be transferred across to the M drive or shared drive to ensure it is backed up.	Portable, enables you to work from different locations. Data is not backed up or secure, and may be lost if the laptop crashes or is stolen.
C drive	Data that the PC user can afford to lose, e.g. reference documents downloaded from the internet.	Data can only be accessed by the PC User. It cannot be accessed outside the office, is not backed up or secure, and may be lost if the computer crashes or is stolen.
M drive	'Work-in-progress', confidential or personal information.	Data can only be accessed by the user. It is backed up.
Shared Drive or Folder	Documents that need to be shared by staff. Information that is not suitable for publication on the intranet/internet and needs to be accessible to staff.	Data is backed up, secure and controlled. Records and information are easily retrieved and access can be controlled easily. Shared storage promotes common practices and reduces duplication.
USB memory stick, CD, DVD, Floppy Disk	Transporting data (e.g. PowerPoint presentations). Sometimes storing back-up copies of non-vital records that do not need to be accessible to more than one person at the same time.	Useful for making back-up copies if you are not on the University network, especially if stored in a separate building. Risk that they may become unreadable and data may be corrupted or lost, so not suitable for long term storage. Also, it is easy to forget about back-up copies when deleting records.
Systems such as VOCAL, SharePoint, VITAL	Collaborative working, sharing information.	Be aware of the purpose of such systems and consider whether your records also need to be held elsewhere. For example, if a system is used to collaborate on a document it may still be necessary to save the final version in another place. Also consider access controls.