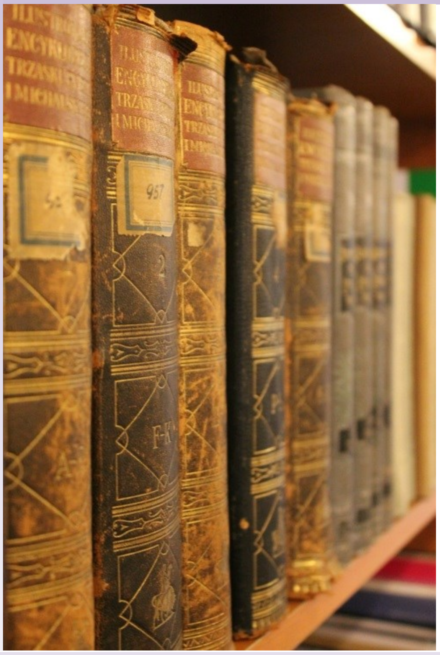
Version 3.0 – August 2017



Preservation

Records Management Factsheet 07

Contents

Introduction 1

Paper records 1

Electronic records 3

Portable media and devices 4

Vital records 5

Historical records 5

Formats 5

Further information 5

Introduction

To ensure a department can operate efficiently, it must preserve its records for as long as access to them is required. Adequate procedures must be in place in order to prevent, for example:

- Information being lost because it has been inadvertently overwritten
- Documents becoming unreadable because they have not been converted to new file formats, but allowed to remain in obsolete technology
- Data being lost because it has become corrupted and has not been backed up
- Data becoming inaccessible because it has been stored on portable media that has degraded
- Data becoming unintelligible because insufficient metadata has been preserved
- Paper records becoming unusable because they have been kept in poor storage conditions and have, for example, become mouldy or brittle

Paper records

An appropriate location must be selected in which to store paper documents. Ideally the immediate office space should be reserved for items that are consulted frequently, while semi-current records (i.e. records referred to occasionally or required to be retained for legal or regulatory reasons) can be kept in separate store rooms. When selecting a room in which to store paper records, it is best to avoid using basements, since they tend to be damp, dusty and are liable to flooding. Departments that need to retain records and do not have sufficient (or suitable) storage space can transfer them off-site. More information can be found on the intranet:
http://www.port.ac.uk/intranet/recordsmanagement/filestore/

Wherever documents are stored, they must be protected from potential hazards.

Fire

Records should be kept away from inflammable materials and ideally stored in metal or fire resistant cabinets. In addition, storage areas should be protected by heat or smoke detection systems and fire resistant doors, which should be kept closed. However, water sprinklers should be avoided, as these can do more damage to paper records than the fire they put out.

Water

Water damage can be caused by floods, burst pipes, poorly maintained drains, gutters and roofs, as well as attempts to extinguish fires. The lowest shelves should always be positioned several centimetres above floor level to protect records in the event of water pooling at floor level. In the case of semi-current records, sturdy cardboard boxes can be used to provide a layer of protection for papers. In the event of mild water damage, it is possible that the contents will remain dry and only the boxes will need to be replaced.

If the risk of water damage in the storage location is high, consideration should be given to the use of archival quality plastic boxes (for example, Really Useful Boxes ™) instead of cardboard. Any records contaminated with sewage must be disposed.

Environmental conditions

Extreme and/or fluctuating levels of temperature and humidity, as well as pockets of stagnant air, are likely to lead to the growth of mould. Storage areas should therefore be adequately ventilated and atmospheric conditions maintained at stable levels. In addition, material should be kept away from outside walls that may be prone to condensation.

Light

Exposure to light will damage paper over time, making it yellow and brittle. Records should be kept away from direct light. Keep lights in storage areas turned off and avoid exposure to sunlight through windows. Storage boxes should be opaque to further restrict light. If records are stored in filing cabinets long term (particularly roll-top cabinets), these should be closed up when not in use.

Pest infestations

To reduce the risk of an infestation of pests (e.g. rodents or insects), storage areas should be cleaned regularly and as far as possible kept free from food. Avoid handling records whilst eating and drinking as organic stains on paper can lead to rapid degradation. Windows should be kept closed to guard against birds and bats. If there is a high risk of an infestation, sticky traps can be used to monitor rooms and ensure that insects etc are discovered as soon as possible. Files which are potentially infested should be quarantined for a period of time to avoid spreading the infestation to other records.

Security

Records containing personal and confidential information must be stored behind two locks (e.g. a locked cabinet in a locked room) when not in use and access only granted to authorised staff. Any rooms that are used to store archived material must similarly be kept locked and the keys held in a secure location.

Personal protection

Records which have been badly damaged by mould, pests or sewage leaks may present a health hazard. Before tackling any significant problem of this sort, it is advisable to conduct a risk assessment and staff working on the records should be provided with suitable protection (e.g. masks and gloves).

Electronic records

Overwriting data

Templates should be available for staff to create routine records, such as minutes, policies, reports, letters and handbooks. Using templates, instead of simply adapting existing documents, will reduce the risk of accidentally erasing previous versions. Particular consideration should also be given to the preservation of dynamic databases (i.e. systems where information is overwritten by new information). If there is likely to be a need to establish what the contents of a database were at a particular time in the past, then a practice of taking periodical snapshots should be introduced.

Within each department there must be procedures and safeguards in place to prevent electronic data from being lost unintentionally or deleted illegitimately.

Access and security

The integrity of electronic data is of paramount importance, if it is considered the primary, definitive record of a transaction. Departments that are responsible for storing records that may be required for evidential purposes should aim to comply with the British Standards Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically; this requires the maintenance of detailed audit trails, allowing all actions to be traced to a person, date and time.

The requirements of staff should be clarified in order to establish who needs to be able to view particular records, who should be able to edit those records and who is entitled to delete them. Appropriate access arrangements can then be put in place to meet these requirements and safeguard data from unauthorised amendments: for example, data can be protected through the use of log-ins, passwords, system access permissions and read-only settings. Encryption should only be used to protect records in transit and only a copy of the original should be encrypted to avoid total loss of the record should the encryption password be forgotten over time.

It should be noted that the application of access controls within an electronic environment will create a maintenance overhead, which must be sustainable and proactively managed. Failure to do so will lead to potential data leakage. It is therefore recommended that effort is focused on:

- Personal and sensitive personal data, as defined by the Data Protection Act 1998
- Commercially confidential data
- Intellectual property

As a general rule, staff should **not** put effort into restricting University access to records which, if requested, would be made publicly available under the Freedom of Information Act 2000.

Metadata

Electronic records require metadata (i.e. data describing the context, content and structure of records) to ensure they can be understood and used efficiently for as long as they are held. The metadata that is to be captured for each type of record should be defined and recorded. Some metadata is automatically captured by software packages. Other metadata may need to be input manually.

The roll out of the EDM system is standardising metadata capture for certain record types. However, basic metadata for records not yet on the EDM system can still be captured via MS Office document properties. The manual capture of metadata brings with it a resource overhead for staff creating the documents. Any metadata fields must therefore be relevant and justifiable.

Backing up

Records must be held on either a relevant corporate system (e.g. EDM system, Student Records system etc) or a networked drive, so that they will be adequately backed up and safeguarded from hardware and software failure. Staff are encouraged to log onto the VPN when away from the University. If this is not feasible, records on laptops should be transferred across to the network at regular intervals, so it will be protected by the University's back up and disaster recovery procedures.

Migration

The longer electronic data is retained, the greater the risk that it could become unreadable. Departments should have procedures in place to ensure that all their records are reviewed periodically and, if necessary, migrated (together with their metadata) to the latest file formats. In particular, it is important to ensure files are not allowed to fall more than two versions behind current software, as backwards compatibility may not be available for older versions. Furthermore, if any records are considered the primary, legal copies, it would be advisable to ensure that the migration procedures comply with the British Standards Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.

If records are expected to be required for a long period of time (e.g. more than ten years), it may be helpful to save them in two formats: one suitable for everyday use (e.g. MS Office Word document) and one suitable for long-term preservation (e.g. PDF/A). PDF/A is an open-source standard (i.e. a standard for which the underlying programming code has been published) designed for long-term storage; it is intended to ensure that the visual appearance of records is preserved, regardless of the systems used for creating or storing the files.

Portable media and devices are <u>not</u> suitable for the long term storage of records

Portable media and devices

Portable media should only ever be used for storing additional copies of records – rather than originals– as there is always a risk of the media degrading. Similarly, portable device hard drives should only be used for keeping data that the user of the PC can afford to lose (e.g. reference documents downloaded from the internet), since it could be irretrievably lost in the event of hardware failure (or theft).

CDs and DVDs

The life-span of a CD or DVD is determined by its handling, the manufacturing quality and environmental conditions. If, for example, it is subjected to careless handling or high levels of humidity and heat, it may last only a couple of years – and, in some cases, only a number of months. It is possible to purchase higher quality CDs and DVDs known as 'archival gold'. These use a dye for the recording layer that is resistant to fading, while the reflective layer is made from gold to protect against corrosion; they also have a thick, protective coating and are better sealed to stop moisture from entering. Archival quality cases are also available; they are made from inert polyester that reduces the risk of damage being caused to the media by chemicals. Archival gold disks are expected to last for decades, provided they are handled carefully. It is, however, always advisable to store important data on the network, so that it will be protected by appropriate back up and disaster recovery procedures. To help to preserve any data that is stored on disks, the following precautions should be taken.

- Keep the disks away from direct sunlight
- Do not leave them in drives unnecessarily as heat or mechanical damage may occur
- Store them in archive quality cases
- Always hold disks by the outer edge or centre to avoid marking the surface with fingerprints or scratches and affecting their readability
- Make at least two copies of each disk and store them in separate and secure locations (i.e. different buildings)
- Check the readability of the data periodically and refresh it (i.e. copy the data onto a new disk) every few years
- Avoid using spindle packs or bulk buys, since they are likely to be of poor quality
- Use disks that only record once, so that the data cannot be changed or overwritten. Rewriting reduces the life expectancy: the more erase-recording cycles to which a disk has been exposed, the shorter its life-span will be.

However, it should be remembered that even if the disk can be preserved for decades, there may no longer be a disk drive into which to put it, or software capable of reading the data on the disk.

USB memory sticks

Memory sticks should only be used for transporting data (e.g. PowerPoint presentations) - not for long-term storage - since there is a danger that they may become unreadable. To safeguard data held on a memory stick, the following precautions should be taken:

- Keep the stick away from magnetic fields, and liquids
- Protect it from extremes of temperature
- Do not touch the electrical contacts and always use the cap to protect them
- Do not leave the device in a PC unnecessarily
- Do not remove the stick from the computer until Windows states it is safe to do so, otherwise the data may become corrupted
- When not in use, keep the device in a secure location

All portable media and devices should be encrypted.
For more information on encryption, contact the IS Service Desk.

Vital records

Records that would be vital to the continued functioning of the University in the event of a disaster (e.g. fire, flood, virus attack) must be identified and protected. Vital records are likely to be irreplaceable or required immediately following a disaster; they will provide information for continuing operations, recreating the University's legal and financial status, preserving its rights, and fulfilling its obligations to its stakeholders.

All critical business data must be stored on a networked drive, so that it will be protected by appropriate back up and disaster recovery procedures. Vital records that are only available in paper format should be duplicated, and the originals and copies stored in separate locations (either in a different building or in off-site storage). If, however, duplication is either impracticable or legally unacceptable, fire proof safes must be used to protect the documents.

Historical records

A small percentage of the University's records are to be preserved permanently because they have long-term reference or historical value. For example, they will provide evidence of the University's most significant functions and activities, document its policy formation, and trace the development of its fabric and infrastructure. The University retention schedules should identify any records with historical value, and further advice can be obtained from the University Archivist.

Formats

As nearly all records are now born-digital (i.e. created on a computer) the preferred method of storage is electronic; although it is acknowledged the some records may have to be retained in paper format. Wherever possible, electronic records should held in open-source, lossless formats (e.g. PDF), especially if they require retention for more than 10 years. For more information on file formats see Factsheet 06: Scanning.

Further information

If you require any further information, please contact the University Records Manager (recordsmanagement@port.ac.uk or ext. 3390) or visit the records management web pages at www.port.ac.uk/records