1. Retention

1.1 Retention refers to the length of time that a category or series of records should be kept for in order to meet operational, business and legal needs.

1.2 A Retention Schedule is a master list that details the timescale specific record types should be retained for.

1.3 The Retention Schedule applies to all records, whether they are held in paper or electronic form.

1.4 A Retention Schedule is an essential tool for achieving organisational efficiency. The schedule identifies the major categories of records, and clarifies the length of time they should be retained for, meaning staff do not need to spend time deciding whether information can be legitimately discarded, they can simply apply the specified retention periods.

1.5 Retention can be complicated if records of a dissimilar nature are filed together (for example where a file contains Record A that needs to be kept for three years and Record B that needs to be kept for six). Departments should consider retention periods when designing their filing systems to avoid this problem. Where this is not possible, files should be weeded regularly to ensure records are not kept too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

1.6 The Data Protection Act requires that personal data be protected from unauthorised destruction, and the Fifth Data Protection Principle states that 'personal data processed for any purpose or purposes shall not be kept for longer than is necessary.' A Retention Schedule is a critical tool in ensuring the law is not breached.

1.7 The Lord Chancellor's Code of Practice on the Management of Records, issued as part of the Freedom of Information Act, states that; 'It is particularly important under FOI that the disposal of records...is undertaken in accordance with clearly established policies which have been formally adopted by authorities and which are enforced by properly authorised staff.' In addition it is a criminal offence under Section 77 of the Freedom of Information Act to erase or destroy any record held by a public authority with the intention of preventing its disclosure. By having clearly defined procedures for the retention and disposal of records, the University can demonstrate that any records that have been destroyed, have been destroyed legitimately in line with standard procedures, and not to prevent disclosure.

2. Disposal

2.1 When a record reaches the end of its retention timescale, a decision must be taken on its disposal.
2.2 There are three potential disposal outcomes for a record reaching the end of its retention timescale:
   a) Reappraisal
   b) Permanent Preservation
   c) Destruction

2.3 **Reappraisal**

2.3.1 It may be that a record needs to be retained beyond the usual timescale because it is, or may be, involved in pending litigation or investigation.

2.3.2 Similarly if records are known to be the subject of a request under Data Protection or Freedom of Information legislation, then any destruction should be delayed. If in doubt contact Information Assurance Services.

2.3.3 If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision. A period of between 6 and 12 months is recommended.

2.4 **Permanent Preservation/Archiving**

2.4.1 Some of the University’s records are retained permanently because they have long term evidential or historical value.

2.4.2 The University’s Retention Schedule should identify records that have archival value. If in doubt contact the University’s Archivist or Information Assurance Services for advice.

2.4.3 Regular arrangements for transfer to the archives should be governed by the agreed retention schedule, although the University’s Archivist may accept one-off transfers under special arrangements.

2.4.4 The following details the main steps to be undertaken when considering transferal of records.

   a) Make contact with the University Archivist. No records can be transferred to the University archives without the prior agreement of the University Archivist.

   b) The University Archivist will advise on the obtaining of archival quality boxes and the quantity required.

   c) The records transfer **must** be accompanied by a transfer list detailing the contents of each box to allow easy retrieval of information, which is to the benefit of the transferring department, as well as the Archivist.

   d) If information contained within any of the records being transferred is not to be made accessible to the public, then the records must be accompanied by a schedule justifying the withholding of that information under the Freedom of Information Act. The schedule should:
      - clearly identify the information you believe should be withheld;
      - cite the reasons for this, making reference to valid exemptions under the Freedom of Information Act where possible; and
      - identify the date after which the release of information may be possible.
e) It should be noted that the decision whether to release information in response to a Freedom of Information, or similar, request will be made by Information Assurance Services. The schedule is for consideration only.

f) If electronic records have been identified as having archival value, then consideration should be given to the following:
   - Are they saved in a format that has been deemed ‘future proof’? If in doubt contact the University’s Archivist or Information Assurance Services for advice.
   - Will they be transferred electronically to the University archives via the network or stored on physical media in order to be transferred (e.g. CD, DVD)?

g) Once records have been received by the Archivist, they will be allocated an accession number. You will be advised of the accession number and should quote it if you require access to records in the future. It is recommended that a copy of the transfer sheet and the accession number is retained and accessible within the department.

2.5 Destruction

2.5.1 The destruction of records should be approved by an authorised person within the department; ideally the Head of Department or a nominated deputy. When authorisation is given, all copies must be destroyed (whether held on paper or electronic media, and whether stored on the network—including on email— or on portable devices such as laptops, USB sticks or smartphones), otherwise the information will be considered still held by the University and therefore accessible under the terms of Freedom of Information and Data Protection legislation.

2.5.2 Paper records containing personal information, or of a confidential, sensitive or restricted nature must be destroyed using the University’s confidential waste service. Steps must be taken to ensure that these records are kept secure whilst awaiting destruction, and a designated member of staff should witness the destruction process.

2.5.3 Electronic records that do not contain confidential, sensitive or restricted information can be simply deleted, although where appropriate you should regularly empty your recycle bin and ‘deleted’ email folders to complete the process.

2.5.4 For electronic records considered to contain confidential, sensitive or restricted information, additional care needs to be taken to ensure that the records are destroyed in a secure manner. In particular the following concerns should be noted:
   - Deletion of a file only removes the link to the file. It does not delete the information within the file. It is therefore possible to use technical measures to reinstate the file.
   - As a consequence of the above, security must continue to be applied to any equipment device that has held such information until such time as it has been securely disposed of or ‘wiped’.
   - Backups of systems will continue to hold copies of the deleted files until such time as the backups are deleted and for which the same security concerns apply.

2.5.5 The above also has implications for data protection and freedom of information legislation. The Information Commissioner has adopted a realistic approach in terms
of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information 'beyond use', and for data protection compliance issues to be 'suspended' provided certain safeguards are in place:

- information has been deleted with no intention on the part of the data controller to use or access this again, but which may still exist in the electronic ether. As such, data protection compliance issues are no longer applicable.
- information that should have been deleted but is in fact still held on a live system because, for technical reasons, it is not possible to delete this information without also deleting other information held in the same batch. It should be noted, however, that in this case a data subject will have the right of access.

2.5.6 The Information Commissioner has also indicated that where information has been 'put beyond use' it will no longer fall within the scope of the legislation. The Information Commissioner will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the person holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible.

2.5.7 It is, however, important to note that where data put beyond use is still held it might need to be provided in response to a court order. Therefore technical solutions should be considered to prevent deletion problems recurring in the future.

2.5.8 It should also be noted that ‘deleted’ information that is still held on a system backup may still be accessible under both the data protection and freedom of information legislation provided it did not require disproportionate effort to retrieve.

2.5.9 For the secure disposal of portable media such as CDs and DVDs the most effective way to eradicate data is to physically destroy the items, preferably using a disk shredder.

2.5.10 For disposal of other equipment please contact IT Services or Information Assurance Services for details of available disposal services.

2.5.11 A record should be kept of what has been destroyed, when and why it was destroyed, and who authorised the destruction. This will ensure there is a transparent audit trail detailing evidence of records that have been destroyed in line with the University’s procedures. A template Record Disposal Form (RM-001) has been created for this purpose.

---

Failure to comply with University Policy may lead to disciplinary action.

---

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.