1. Record Types

1.1 Various types of record can be created, and their format is irrelevant, be it paper, electronic, photographic etc. Examples of record types include:

- **Permanent Records**: These will be needed for as long as the institution is in existence either as a permanent legal requirement or as part of an historical archive e.g. minutes of important committees, audited annual accounts.

- **Time-limited**: Records containing details of current information that are used and updated on a daily, weekly or monthly basis etc. When they are no longer needed for operational purposes they may need to be maintained for a period of time with retention periods being applied to this phase.

- **Transactional**: These are usually contained within electronic systems, and provide an audit trail of changes, usually through processed information.

- **Vital**: Records which are irreplaceable and do not have the same value (legal or evidential) if reproduced.

- **Important**: Records which if lost or destroyed can be retrieved from another source but only after considerable delay and at some expense.

- **Useful**: Would cause inconvenience if lost but could be easily replaced.

- **Non-essential**: Records which can be destroyed without significant harm.

- **Active**: Records which must be referred to regularly—both in the context of the record itself and the record series as a whole. Normally quick access to the records is required.

- **Semi-active**: Records that are referred to on an occasional basis. The need for the record may diminish over time. Normally quick access is not required and it does not need to be stored locally for the department to carry out its functions.

- **Inactive**: A record that is seldom, if ever, referred to or inspected.

- **Permanent Records**: Are records of long term historical or research value that are retained permanently in an office or in the archives after a period of active use (also called archival records)

1.2 It is essential that information is captured in a way that ensures it can be accessed efficiently at a later date. Appropriate record creation, filing schemes, access policies and tracking systems are the key to ensuring this occurs.

1.3 **Filing scheme**

1.3.1 A file is essentially a storage place for information. When deciding upon the value of a file its format is irrelevant.

1.3.2 A filing scheme is used as a framework for organising records within a hierarchy. It applies to all records. It should include a set of rules for referencing, titling,
indexing and, if appropriate, security marking of records. It promotes consistency ensuring that the same kind of information is called by the same name.

1.3.3 Records should be arranged and described in a manner that facilitates fast, accurate and comprehensive retrieval so that records are accessible to those who require them.

1.3.4 Records may be retained in a records series. A records series is a group or unit of related records, documents or information that is normally filed or kept together because they relate to a particular subject or function, result from the same activity or document a particular transaction or activity.

1.3.5 Both paper and electronic record keeping systems should contain metadata (descriptive and technical documentation) to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records. The metadata file should contain information about the scheme itself: structure, dates of usage, details of alterations, deletions etc.

1.3.6 Individuals should be identified within units to take responsibility for master versions of documents to avoid unnecessary long-term retention of duplicates.

1.3.7 To reduce the need for duplication and where practicable documents should be stored in central folders that are accessible by staff. Similarly, electronic information should be filed in shared corporate workspaces wherever possible.

1.3.8 File titles should be brief but comprehensible, and a consistent format should be used.

1.4 Access policy

1.4.1 An Access Policy should be produced to identify who is allowed to have access to which records and to highlight if special security measures are required for any records.

1.4.2 All records must be kept appropriately secure as befits the confidentiality and importance of the record, and records should be protected from non-authorised disclosure.

1.4.3 Care must be exercised in the handling of all records and they should be returned to designated storage promptly after use.

1.5 Tracking and monitoring systems

1.5.1 The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

1.5.2 Where a record is loaned to another person, department or external organisation, this should be recorded so that the whereabouts of the record can be tracked using manual or electronic systems.

1.6 Storage arrangements

1.6.1 Records should be stored in a safe and secure physical and electronic environment. There are four stages in the storage requirements of records:

- **Active:** Records that have recently been created, or are in current use, will normally be stored as close to the user as possible. When no longer required
for immediate use some records may be destroyed, while others will be moved into short-term storage.

- **Semi-active:** When a record is no longer required for immediate use, it will normally be stored where it can be retrieved within 24 hours. It is the responsibility of departments to identify suitable space for the short-term storage of departmental records.

- **Inactive:** When a record has reached a point where it rarely or never needs to be accessed, but the University still needs to retain it, it will be moved to long term storage. Retrieval of such records may be costly/time consuming.

- **Permanent Records:** Are records of long term historical or research value that are retained permanently in an office or in the archives after a period of active use (also called archival records)

1.6.2 Storage accommodation for records should be clean and tidy. It should prevent damage to the records, protect against unauthorised access and meet fire regulations, whilst allowing maximum accessibility to the information commensurate with its frequency of use.

1.6.3 Procedures for handling records should take full account of the need to preserve important information. Records should be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability.

1.6.4 All records in whatever format must be held securely in accordance with the requirements of the Information Security Policy. When storing confidential or very important records consideration should be given to whether rooms should have one or more of the following: barred/secure windows, secure doors, guards or intruder alarms, controlled access key system, fire protection, humidity protection, protection against water damage and protection from contaminants.

1.6.5 In line with the retention schedule, and point 2.5.1 above, records retained up to the end of their lifecycle will fall into one of three groups below, a, b and c. As time passes a record should move from category a to b, and then to c. Records will then either be transferred to the category d where a permanent record is required, or destroyed if no longer required.

a) Records that need to be accessed on a regular basis, i.e. daily/weekly.
b) Records that need to be accessed moderately frequently, i.e. monthly/annually.
c) Records that need to be accessed rarely or never, yet still need to be retained.
d) Permanent archive

1.6.6 Where storage space is an issue the use of a third party offsite storage company may be considered. Whilst this can be a cost effective way of managing records the use of such a company should always be preceded by seeking advice from Information Assurance Services.

1.6.7 Careful thought should be given to the types of records that are selected for offsite storage, in particular to how quickly such records may need to be accessed, and also how frequently. There are usually additional costs for retrieval of records, and so the more often records are needed the more expensive storage will be. In addition it can sometimes take several days to get a record back from an offsite provider, with quicker retrievals incurring higher costs. Therefore it is
recommended that wherever possible records selected for offsite storage should be those which fall into category c or d as specified within 2.5.5.

1.6.8 All third party organisations should be subject to a full risk assessment before the agreement of any contract. This is to ensure their facilities meet suitable requirements for security and offer protection against damage from fire, flood etc.

1.7 **Scanning**

1.7.1 Scanning, if undertaken properly and for the right reasons, can make information more accessible and reduce the amount of physical space taken up by paper records, but it is not a panacea. Used inappropriately it can have serious cost and legal implications. Advice should always be sought from Information Assurance Services.

1.7.2 Scanning is not a substitute for good records management and in particular the following should be carefully considered before scanning is undertaken.

- Scanning can be costly. If space is an issue and the records are rarely needed then offsite storage might be a more cost effective solution.
- It is unsuitable for a series of records to which information is still being added.
- Scanning a document may reduce or even negate its evidential weight. This is particularly true of records relating to legal or financial matters.
- It can make it harder to preserve records unless care is taken to ensure the scans are created using appropriate file formats.

2. **How long records should be kept**

2.1 Whilst information must be organised so that it can be accessed as efficiently as possible, it is also important to ensure that it is kept only as long as it is necessary.

2.2 **Retention schedule**

2.2.1 The University’s Records Retention Schedule applies to all formats of records, and identifies how long particular records should be kept.

2.2.2 It promotes consistency – the same types of record are kept for the same length of time – and ensures the retention of the minimum volume of records. It aids compliance with Data Protection and Freedom of Information legislation and also research funding bodies’ requirements.

2.2.3 Where records are identified that are not referenced by the retention schedule, it should be referred to Information Assurance Services who will determine a suitable retention timescale for the records and update the retention schedule accordingly.

2.3 **Records closure and disposal procedures**

2.3.1 Departments should have in place systems for managing the regular appraisal of records by referencing the University’s Retention Schedule and for recording the disposal decisions made. Records should be closed as soon as they have ceased to be of active use other than for reference purposes. An indication that a file of paper records or folder of electronic records has been closed should be shown on the record itself. Wherever possible, information on the intended disposal of electronic records should be included in the metadata when the record is created.
2.3.2 The functions from which records are likely to be selected for permanent preservation and the periods for which other records should be retained are set out in the University's records retention schedule.

2.3.3 Records selected for permanent preservation and no longer in regular use should be transferred as soon as possible to the University Archive.

2.3.4 Records that have outlived their administrative usefulness and have not been selected for permanent preservation should be destroyed in as secure a manner as is necessary for the level of confidentiality they bear in accordance with the retention schedule.

2.3.5 A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved.

2.3.6 Care must be taken if destroying any data associated with a DPA or FOIA case/enquiry, or data associated with any formal or legal investigation or which may be required to be kept by an external funding body.

2.4 Vital records programme

2.4.1 A contingency or business recovery plan should be in place to provide protection against loss and destruction for records which are vital to the continued functioning of the University. Vital records should be identified and a preservation and recovery strategy put in place. Suitable back up procedures should be in place in the event of a disaster. Reference should be made to Business Continuity and Disaster Recovery procedures.

2.5 Archives

2.5.1 The Records Retention schedules contain details of the records that should be transferred to the archives. Broadly speaking the following records may be worthy of permanent preservation:

- Records that document policy formation
- Records that show the development of the University’s fabric and infrastructure
- Records that show evidence of important decisions or precedent
- Records showing the development of the relationship between the students, the academic departments and the administrative departments
- Records that show the development of academic departments
- Papers relating to the University’s charter, statutes, ordinances & regulations; Court, Council, Senate agendas minutes & supporting papers; Council & Senate committees agendas & papers; published reports & documents; promotional material; plans & photographs of buildings

3. Ensuring records remain accessible over time

3.1 Preservation Strategy

3.1.1 A preservation strategy should be in place to ensure that records remain accessible over time. The preservation strategy should cover all types of record including electronic records and should ensure that records to be kept for long-term retention to meet administrative, statutory and historical needs are not lost by media deterioration and obsolescence. Records and their conceptual metadata should be stored in such a way as to prevent future modification or deletion by
users. Electronic data and metadata should be preserved in a format that is independent of proprietary hard and software.

**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.