Records Retention Schedule for Information & Communications Technology [ICT] Management

This category is intended to cover all ICT systems in the institution, regardless of which business units are involved in developing, operating or using the systems.

This retention schedule is based on the recommendations made by the Joint Information Systems Committee. The letter indicates the final disposition of each type of record, and applies to original records. Where copies of originals are kept locally, these can be destroyed when these are no longer required.:

A = 1 copy to be transferred to the University Archive. See Retention Schedule Guidelines for further details.

D = Destroyed.

The number following the letter code indicates the period (in years) after which records may be destroyed, and is the minimum retention period required by best practice or legislation. It assumes a new file is opened at the start of each academic, calendar or financial year, and is **always** calculated from the date of the last record in the file.

FOLDER STRUCTURE	Examples of Types of Record	Retention Period	Legislative Authority
ICT/STRATEGY • identifying requirements for new/revised strategy • undertaking research • developing strategy proposals • consulting on strategy proposals • reviewing and revising strategy proposals in the light of comments received • drafting strategy documents • consulting on strategy documents • reviewing draft strategy documents in the light of comments received • producing final strategy documents • submitting final strategy documents for formal endorsement • formally endorsing strategy documents • disseminating strategy documents • reviewing strategy.	Key records documenting the development and establishment of the institution's ICT management strategy. Working papers documenting development and establishment of the institution's ICT management strategy.	A: Superseded + 5 years Copy to the University Archive after approval for permanent retention. D: Issue of strategy + 1 year	

ICT/POLICY • identifying requirements for new/revised policy • undertaking research • developing policy proposals • consulting on policy proposals • reviewing and revising policy proposals in the light of comments received • drafting policy documents • consulting on policy documents • reviewing draft policy documents in the light of comments received • producing final policy documents • submitting final policy documents for formal approval • formally approving policy documents • disseminating policy documents • reviewing policy	Key records documenting the development and establishment of the institution's ICT management policies. Working papers documenting development and establishment of the institution's ICT management policies.	A: Superseded + 5 years Copy to the University Archive after approval for permanent retention. D: Issue of policy + 1 year	
ICT/PROCEDURES • identifying needs for new/revised procedure • undertaking research • analysing work processes • drafting procedure documents • consulting on procedure documents • reviewing draft procedure documents in the light of comments received • trialling procedure • refining procedure as a result of trials • submitting final procedure documents for formal approval • formally approving procedure documents • disseminating procedure documents • reviewing procedure.	Master copies of procedures relating to ICT management. Development of the institution's procedures relating to ICT management.	A: Superseded + 3 years Copy to the University Archive after approval for permanent retention. D: Issue of procedures + 1 year	

Records Retention Schedule for Information & Communications Technology [ICT] Management (3)

ICT/SYSTEMS/DEVELOPMENT • specifying requirements • evaluating potential systems/solutions • installing systems • testing systems • commissioning systems • controlling changes to systems • decommissioning systems.	Initial development and post-implementation modification and maintenance of ICT systems. Iinitial development of ICT systems which are not implemented. Management of ICT systems development projects (i.e. project management records).	D: Decommissioning of system + 5 years D: Last action on development + 5 years D: Termination of project + 5 years	
ICT/SYSTEMS/OPERATIONS • monitoring system performance • reporting, investigating and resolving system faults • managing system data storage, including backup, migration, archiving and deletion • maintaining appropriate system software licences.	Routine monitoring and testing of the operation of ICT systems, and action taken to rectify problems and optimise performance. Faults reported by users of ICT systems, and action taken to investigate and resolve the problem. Management of system data storage, including the operation of routine data backup, archiving and deletion routines. User requests to recover data from backup or archive stores, and action taken. Maintenance of appropriate software licences for live ICT systems.	D: Current year + 1 year D: Last action on fault + 1 year D: Current year + 1 year D: Last action on request + 3 months D: Issue of new licence	

ICT/SYSTEMS/SECURITY		
• opening and closing system user accounts • monitoring use of systems to ensure compliance with institutional policies and relevant legislation • responding to security breaches or incidents • sanitisation of ICT hardware before disposal.	Security arrangements for ICT systems.	D: Decommissioning of system + 5 years
	Opening, maintenance and closure of user accounts for ICT systems.	D: Closure of account + 1 year
	Routine monitoring of the use of ICT systems to ensure compliance with legal requirements and institutional policies.	D: Current year + 1 year
	Attempted or actual security breaches of the institution's ICT systems, and action taken.	D: Last action on incident + 1 year
	Requests for, and authorisation of, connections of third party equipment to the institution's networks, either on institutional premises or via dial-up communications links.	D: Termination of connection + 1 year
	Removal/return of mobile ICT systems hardware and software from/to the institution's premises.	D: Return of equipment + 3 months
	Arrangements for the sanitisation of institutional ICT equipment prior to disposal.	D: Disposal of equipment + 1 year

ICT/SYSTEMS/TRAINING • identifying training requirements • identifying and evaluating training options. For external training, activities include: • identifying and evaluating training programmes • organising attendance at training events • evaluating training programmes/events. For internal training, activities include • developing training programmes • organising and arranging training events • delivering training • evaluating training programmes/events.	Development of technical and application training for ICT system users.	D: Superseded + 1 year	